

Security and Privacy Controls Applicable to Enhanced Direct Enrollment (EDE) Entities

Security/Privacy Control	Control #	Security/Privacy Control Name	EDEs (PY 2020)	EDE ISCM Core Control	CIS Critical Security Controls (CSC)	Corresponding HIPAA Security Rule	45 CFR 155.260 Mapping	Cybersecurity Framework (CSF v 1.1) Mapping	ISCM Timelines
Access Control (AC)	AC-1	Access Control Policy and Procedures	X	X	CSC-14	164.306,	(a)(1)(iii)(A),	ID.GV-1	3 years
Access Control (AC)	AC-2	Account Management	X	X	CSC-4, CSC-14, CSC-16	164.308(a)(1)(ii)(D),		PR.AC-1	Continuous and Ongoing
Access Control (AC)	AC-2(1)	Automated System Account	X			164.308(a)(1)(ii)(D),			
Access Control (AC)	AC-2(2)	Removal of Temporary/Emergency	X			164.308(a)(1)(ii)(D),			24 hours
Access Control (AC)	AC-2(3)	Disable Inactive Accounts	X			164.308(a)(1)(ii)(D),			60 days
Access Control (AC)	AC-2(4)	Automated Audit Actions	X			164.308(a)(1)(ii)(D),			
Access Control (AC)	AC-2(5)	Inactivity Logout							
Access Control (AC)	AC-2(7)	Role-Based Schemes	X			164.308(a)(1)(ii)(D),			Continuous and Ongoing
Access Control (AC)	AC-2(9)	Restrictions On Use Of Shared/Group							
Access Control (AC)	AC-2(10)	Shared / Group Account Credential	X			164.308(a)(1)(ii)(D),			
Access Control (AC)	AC-2(12)	Account Monitoring / Atypical Usage							
Access Control (AC)	AC-3	Access Enforcement	X	X	CSC-13, CSC-14, CSC-16	164.308(a)(3),	(a)(3)(vi), (a)(4)(ii),	PR.AC-4	
Access Control (AC)	AC-3(9)	Access Enforcement – Controlled				164.308(a)(1)(ii)(D),	(a)(1)(iii)(A),		
Access Control (AC)	AC-4	Information Flow Enforcement	X		CSC-9, CSC-11, CSC-12, CSC-	164.308(a)(1)(ii)(A),		ID.AM-3	
Access Control (AC)	AC-4(21)	Access Only							
Access Control (AC)	AC-5	Separation of Duties	X	X		164.308(a)(1)(ii)(D),		PR.AC-4	
Access Control (AC)	AC-6	Least Privilege	X	X	CSC-4, CSC-14	164.308(a)(1)(ii)(D),	(a)(1), (a)(1)(i),	PR.AC-4	
Access Control (AC)	AC-6(1)	Authorize Access to Security	X			164.308(a)(1)(ii)(D),			
Access Control (AC)	AC-6(2)	Non-Privileged Access for Non-	X			164.308(a)(1)(ii)(D),			
Access Control (AC)	AC-6(5)	Privileged Accounts	X			164.308(a)(1)(ii)(D),			
Access Control (AC)	AC-6(9)	Auditing Use of Privileged Functions	X			164.308(a)(1)(ii)(D),			
Access Control (AC)	AC-6(10)	Prohibit Non-Privileged Users from	X			164.308(a)(1)(ii)(D),			
Access Control (AC)	AC-7	Unsuccessful Logon Attempts	X		CSC-16			PR.AC-7	
Access Control (AC)	AC-7	Unsuccessful Logon Attempts	X					PR.AC-7	
Access Control (AC)	AC-8	System Use Notification	X					PR.AC-7	
Access Control (AC)	AC-9	Previous Logon (Access) Notification						PR.AC-7	
Access Control (AC)	AC-10	Concurrent Session Control	X	X				PR.AC-5	
Access Control (AC)	AC-11	Session Lock	X	X	CSC-16	164.312(a)(1);		PR.AC-7	
Access Control (AC)	AC-11(1)	Pattern-Hiding Displays	X						
Access Control (AC)	AC-12	Session Termination	X	X	CSC-16	164.312(a)(2)(iii);		PR.AC-7	
Access Control (AC)	AC-13	Supervision and Review - Access							
Access Control (AC)	AC-14	Permitted Actions Without	X					PR.AC-7	
Access Control (AC)	AC-15	Automated Marking							
Access Control (AC)	AC-16	Security Attributes				164.308(a)(3),		PR.AC-6	
Access Control (AC)	AC-17	Remote Access	X	X	CSC-4, CSC-12	164.308(a)(1)(ii)(D),		PR.AC-3	365 days/Annually
Access Control (AC)	AC-17(1)	Automated Monitoring/Control	X			164.308(a)(1)(ii)(D),			
Access Control (AC)	AC-17(2)	Protection of Confidentiality/Integrity	X			164.308(a)(1)(ii)(D),			
Access Control (AC)	AC-17(3)	Managed Access Control Points	X			164.308(a)(1)(ii)(D),			
Access Control (AC)	AC-17(4)	Privileged Commands/Access	X			164.308(a)(1)(ii)(D),			
Access Control (AC)	AC-17(9)	Disconnect / Disable Access	X						
Access Control (AC)	AC-18	Wireless Access	X		CSC-15	164.308(a)(1)(ii)(D),		PR-PT-4	
Access Control (AC)	AC-18(1)	Authentication and Encryption	X			164.308(a)(1)(ii)(D),			
Access Control (AC)	AC-19	Access Control for Mobile Devices	X		CSC-4, CSC-15	164.308(a)(4)(i),		PR.AC-3	
Access Control (AC)	AC-19(5)	Full-Device / Container-Based	X			164.308(a)(4)(i),			
Access Control (AC)	AC-20	Use of External Information Systems	X		CSC-12	164.308(a)(4)(i),	(a)(1)(iii)(A),	ID.AM-4	
Access Control (AC)	AC-20(1)	Limits on Authorized Use	X			164.308(a)(4)(i),			
Access Control (AC)	AC-20(2)	Portable Storage Devices	X			164.308(a)(4)(i),			
Access Control (AC)	AC-21	Information Sharing	X			164.308(a)(3)(ii)(A);	(a)(1)(iii),	PR.IP-8	
Access Control (AC)	AC-22	Publicly Accessible Content	X			164.502(a)			90 days/Quarterly
Access Control (AC)	AC-23	Data Mining Protection			CSC-6, CSC-13				
Access Control (AC)	AC-24	Access Control Decisions			CSC-14			PR.AC-6	
Access Control (AC)	AC-25	Reference Monitor						DE.DP-2	
Awareness and	AT-1	Security Awareness and Training	X		CSC-17	164.306,	(b)(3)(iii)	ID.GV-1	3 years
Awareness and	AT-2	Security Awareness Training	X		CSC-17	164.308(a)(5)(ii)	(c)	PR.AT-1	365 days/Annually

Awareness and	AT-2(2)	Insider Threat	X			164.308(a)(5)	(c)		
Awareness and	AT-3	Role-Based Security Training	X		CSC-17	164.308(a)(2),		PR.AT-4	365 days/Annually
Awareness and	AT-4	Security Training Records	X		CSC-17	164.308(a)(5)(i);			
Awareness and	AT-5	Contacts with Security Groups and							
Audit and	AU-1	Audit and Accountability Policy and	X			164.306,	(a)(3)(viii), (b)(3)(i),	ID.GV-1	365 days/Annually
Audit and	AU-2	Audit Events	X	X	CSC-6	164.308(a)(1)(ii)(D),	(a)(3)(vi),	PR.PT-1	
Audit and	AU-2(3)	Reviews and Updates	X			164.308(a)(1)(ii)(D),	(a)(3)(viii), (b)(3)(i),		365 days/Annually
Audit and	AU-3	Content of Audit Records	X		CSC-6	164.308(a)(1)(ii)(D),	(a)(3)(vi), (b)(3)(i)	PR.PT-1	
Audit and	AU-3(1)	Additional Audit Information	X			164.308(a)(1)(ii)(D),			
Audit and	AU-4	Audit Storage Capacity	X		CSC-6	164.308(a)(1)(ii)(A),		PR.PT-1	
Audit and	AU-5	Response to Audit Processing Failures	X		CSC-6	164.308(a)(1)(ii)(D),		PR.PT-1	
Audit and	AU-5(1)	Audit Storage Capacity	X			164.308(a)(1)(ii)(D),			
Audit and	AU-6	Audit Review, Analysis, and Reporting	X	X	CSC-6	164.308(a)(1)(i),	(a)(3)(vi),	PR.PT-1	Continuous and Ongoing
Audit and	AU-6(1)	Process Integration	X			164.308(a)(1)(i),			
Audit and	AU-6(3)	Correlate Audit Repositories	X			164.308(a)(1)(i),			
Audit and	AU-7	Audit Reduction and Report	X		CSC-6	164.308(a)(1)(ii)(D),		PR.PT-1	
Audit and	AU-7(1)	Automatic Processing	X			164.308(a)(1)(ii)(D),			
Audit and	AU-8	Time Stamps	X		CSC-6	164.308(a)(1)(ii)(D),		PR.PT-1	
Audit and	AU-8(1)	Synchronization with Authoritative	X			164.308(a)(1)(ii)(D),			
Audit and	AU-9	Protection of Audit Information	X		CSC-6	164.306(a)(1);	(a)(3)(viii), (b)(3)(i)	PR.PT-1	
Audit and	AU-9(2)	Audit Backup On Separate Physical							
Audit and	AU-9(4)	Access by Subset of Privileged Users	X			164.308(a)(1)(ii)(D),			
Audit and	AU-10	Non-Repudiation	X		CSC-6	164.308(a)(1)(ii)(D),	(a)(3)(vi),	PR.PT-1	
Audit and	AU-11	Audit Record Retention	X		CSC-6	164.308(a)(1)(ii)(D),	(a)(3)(viii), (b)(3)(i)	PR.PT-1	
Audit and	AU-12	Audit Generation	X		CSC-6	164.308(a)(1)(ii)(D),	(a)(3)(viii), (b)(3)(i)	PR.PT-1	
Audit and	AU-12(1)	System-Wide/Time-Correlated Audit				164.308(a)(1)(ii)(D),	(a)(3)(viii), (b)(3)(i)		
Audit and	AU-13	Monitoring for Information			CSC-6	164.308(a)(1)(ii)(D),		DE.CM-3	
Audit and	AU-14	Session Audit			CSC-6				
Audit and	AU-15	Alternate Audit Capability							
Audit and	AU-16	Cross-Organizational Auditing				164.308(a)(1)(ii)(D),			
Security Assessment	CA-1	Security Assessment and	X			164.306,	(a)(5), (b)(2)(iii),	ID.GV-1	3 years
Security Assessment	CA-2	Security Assessments	X		CSC-3, CSC-20	164.308(a)(6)(ii),	(a)(5), (b)(2)(iii),	DE.DP-1	365 days/Annually
Security Assessment	CA-2(1)	Independent Assessors	X			164.308(a)(6)(ii),			
Security Assessment	CA-2(2)	Specialized Assessments							
Security Assessment	CA-2(3)	External Organizations							
Security Assessment	CA-3	System Interconnections	X	X	CSC-11, CSC-12, CSC-15	164.308(a)(1)(ii)(A),	(a)(6), (b)(3)(i)	ID.AM-3	
Security Assessment	CA-3(3)	Unclassified Non-National Security				164.312(a)(1)			
Security Assessment	CA-3(5)	Restrictions on External System	X			164.308(a)(1)(ii)(A),			
Security Assessment	CA-4	Security Certification							
Security Assessment	CA-5	Plan of Action and Milestones	X	X	CSC-20				30 days / or within one month
Security Assessment	CA-5(1)	Automation Support for							
Security Assessment	CA-6	Security Authorization	X		CSC-20	164.308(a)(2);			365 days/Annually
Security Assessment	CA-7	Continuous Monitoring	X		CSC-1, CSC-2, CSC-3, CSC-4,	164.306(e),	(a)(3)(viii), (a)(5),	DE.CM-1	365 days/Annually
Security Assessment	CA-7(1)	Independent Assessment	X			164.306(e),			365 days/Annually
Security Assessment	CA-8	Penetration Testing	X		CSC-20	164.308(a)(1)(ii)(A),		ID.RA-1	365 days/Annually
Security Assessment	CA-8(1)	Independent Penetration Agent or	X						
Security Assessment	CA-9	Internal System Connections	X		CSC-9, CSC-11, CSC-12, CSC-	164.308(a)(1)(ii)(A),		ID.AM-3	
Configuration	CM-1	Configuration Management Policy	X			164.306,	(b)(3)(iii)	ID.GV-1	3 years
Configuration	CM-2	Baseline Configuration	X	X	CSC-2, CSC-5, CSC-7, CSC-9,	164.308(a)(4)*		DE.AE-1	
Configuration	CM-2(1)	Reviews and Updates	X			164.308(a)(4)*			365 days/Annually
Configuration	CM-2(2)	Automation Support for							
Configuration	CM-2(3)	Retention of Previous Configurations	X			164.308(a)(4)*			
Configuration	CM-2(7)	Configure Systems, Components, or							
Configuration	CM-3	Configuration Change Control	X	X	CSC-5, CSC-7, CSC-11	164.308(a)(7)(i),	(b)(2)(iv)	DE.CM-1	Continuous and Ongoing
Configuration	CM-3(2)	Test/Validate/Document Changes	X			164.308(a)(7)(i),			
Configuration	CM-4	Security Impact Analysis	X	X		164.308(a)(1)(ii)(A);		PR.IP-1	
Configuration	CM-4(1)	Separate Test Environments	X			164.308(a)(7)(i),			
Configuration	CM-4(2)	Verification of Security Functions				164.308(a)(7)(i),			
Configuration	CM-5	Access Restrictions for Change	X		CSC-5, CSC-7, CSC-11	164.308(a)(7)(i),		PR.IP-1	

Configuration	CM-5(1)	Automated Access	X						
Configuration	CM-5(3)	Signed Components							
Configuration	CM-5(5)	Limit Production/Operational	X			164.308(a)(7)(i),			90 days/Quarterly
Configuration	CM-6	Configuration Settings	X	X	CSC-5, CSC-7, CSC-9, CSC-11	164.308(a)(7)(i),		PR.IP-1	Continuous and Ongoing
Configuration	CM-6(1)	Automated Central Management/	X			164.308(a)(7)(i),			
Configuration	CM-7	Least Functionality	X	X	CSC-5, CSC-7	164.308(a)(7)(i),		PR.PT-3	
Configuration	CM-7(1)	Periodic Review	X			164.308(a)(7)(i),			90 days/Quarterly
Configuration	CM-7(2)	Prevent Program Execution	X	X		164.308(a)(7)(i),			
Configuration	CM-7(4)	Unauthorized Software/Blacklisting	X	X		164.308(a)(7)(i),			90 days/Quarterly
Configuration	CM-7(5)	Authorized Software / Whitelisting							
Configuration	CM-8	Information System Component	X		CSC-1, CSC-2, CSC-5, CSC-7,	164.308(a)(1)(ii)(A),		ID.AM-1	Continuous and ongoing
Configuration	CM-8(1)	Updates During	X			164.308(a)(1)(ii)(A),			Continuous and ongoing
Configuration	CM-8(3)	Automated Unauthorized Component	X			164.308(a)(1)(ii)(A),			Continuous and ongoing
Configuration	CM-8(5)	No Duplicate Accounting of	X			164.308(a)(1)(ii)(A),			
Configuration	CM-9	Configuration Management Plan	X		CSC-5, CSC-7	164.308(a)(7)(i),		PR.IP-1	
Configuration	CM-10	Software Usage Restrictions	X		CSC-2	164.308(a)(1)(ii)(D),		DE.CM-3	
Configuration	CM-10(1)	Open Source Software	X			164.308(a)(1)(ii)(D),			
Configuration	CM-11	User-Installed Software	X		CSC-2, CSC-5, CSC-7	164.308(a)(1)(ii)(D),		DE.CM-3	
Contingency	CP-1	Contingency Planning Policy and	X			164.306,	(b)(3)(iii)	ID.GV-1	3 years
Contingency	CP-2	Contingency Plan	X			164.308(a)(2),		ID.AM-5	365 days/Annually
Contingency	CP-2(1)	Coordinate with Related Plans	X			164.308(a)(2),			
Contingency	CP-2(2)	Capacity Planning	X			164.308(a)(2),			
Contingency	CP-2(3)	Resume Essential Missions/Business	X			164.308(a)(2),			
Contingency	CP-2(8)	Identify Critical Assets	X			164.308(a)(2),			
Contingency	CP-3	Contingency Training	X					RS.CO-1	365 days/Annually
Contingency	CP-4	Contingency Plan Testing	X			164.308(a)(7)(ii)(A)		PR.IP-4	365 days/Annually
Contingency	CP-4(1)	Coordinate with Related Plans	X			164.308(a)(7)(ii)(A),			
Contingency	CP-5	Contingency Plan Update							
Contingency	CP-6	Alternate Storage Site	X			164.308(a)(7)(ii)(A),		PR.IP-4	
Contingency	CP-6(1)	Separation from Primary Site	X			164.308(a)(7)(ii)(A),			
Contingency	CP-6(3)	Accessibility	X			164.308(a)(7)(ii)(A),			
Contingency	CP-7	Alternate Processing Site						PR.IP-9	
Contingency	CP-7(1)	Separation from Primary Site							
Contingency	CP-7(2)	Accessibility							
Contingency	CP-7(3)	Priority of Service							
Contingency	CP-8	Telecommunications Services	X			164.308(a)(1)(ii)(D),		ID.BE-4	
Contingency	CP-8(1)	Priority of Service Provisions	X			164.308(a)(1)(ii)(D),			
Contingency	CP-8(2)	Single Points of Failure	X			164.308(a)(1)(ii)(D),			
Contingency	CP-9	Information System Backup	X		CSC-10	164.308(a)(7)(ii)(A);		PR.IP-4	
Contingency	CP-9(1)	Testing for Reliability/Integrity	X			164.308(a)(7)(ii)(A),			6 months
Contingency	CP-9(3)	Separate Storage For Critical							
Contingency	CP-10	Information System Recovery and	X		CSC-10	164.308(a)(6)(ii),			
Contingency	CP-10(2)	Transaction Recovery	X			164.308(a)(6)(ii),			
Contingency	CP-11	Alternate Communications Protocols				164.308(a)(1)(ii)(B),		ID.BE-5	
Contingency	CP-12	Safe Mode						PR.IP-9	
Contingency	CP-13	Alternative Security Mechanisms						PR.IP-9	
Identification and	IA-1	Identification and Authentication	X			164.306,	(a)(4)(ii), (b)(3)(i),	ID.GV-1	3 years
Identification and	IA-2	Identification and Authentication	X	X	CSC-4	164.308(a)(3)(ii)(B),	(a)(4)(ii), (b)(3)(i)	PR.AC-1	
Identification and	IA-2(1)	Network Access to Privileged	X	X		164.308(a)(3)(ii)(B),	(a)(4)(ii), (b)(3)(i)		
Identification and	IA-2(2)	Network Access to Non-Privileged	X	X		164.308(a)(3)(ii)(B),	(a)(4)(ii), (b)(3)(i)		
Identification and	IA-2(3)	Local Access to Privileged Accounts	X			164.308(a)(3)(ii)(B),	(a)(4)(ii), (b)(3)(i)		
Identification and	IA-2(5)	Group Authentication							
Identification and	IA-2(8)	Network Access to Privileged	X			164.308(a)(3)(ii)(B),	(a)(4)(ii), (b)(3)(i)		
Identification and	IA-2(11)	Remote Access – Separate Device	X			164.308(a)(3)(ii)(B),	PR.AC-1		
Identification and	IA-2(12)	Acceptance of PIV Credentials							
Identification and	IA-3	Device Identification and	X		CSC-1, CSC-15,	164.308(a)(3)(ii)(B),	(a)(4)(ii), (b)(3)(i)	PR.AC-1	
Identification and	IA-4	Identifier Management	X		CSC-4	164.308(a)(3)(ii)(B),	(a)(4)(ii), (b)(3)(i)	PR.AC-1	3 years
Identification and	IA-4	Identifier Management	X					PR.AC-1	60 days
Identification and	IA-4 (4)	Identify User Status							

Identification and	IA-5	Authenticator Management	X	X	CSC-4, CSC-16	164.308(a)(3)(ii)(B),	(a)(4)(ii), (b)(3)(i)	PR.AC-1	60 days
Identification and	IA-5(1)	Password-Based Authentication	X	X		164.308(a)(3)(ii)(B),	(a)(4)(ii), (b)(3)(i)		
Identification and	IA-5(2)	PKI-Based Authentication	X			164.308(a)(3)(ii)(B),	(a)(4)(ii), (b)(3)(i)		
Identification and	IA-5(3)	In-Person or Trusted Third-Party	X			164.308(a)(3)(ii)(B),	(a)(4)(ii), (b)(3)(i)		
Identification and	IA-5(4)	Automated Support For Password							
Identification and	IA-5(6)	Protection of Authenticators							
Identification and	IA-5(7)	No Embedded Unencrypted Static	X			164.308(a)(3)(ii)(B),	(a)(4)(ii), (b)(3)(i)		
Identification and	IA--5(11)	Hardware Token-Based	X			164.308(a)(3)(ii)(B),	(a)(4)(ii), (b)(3)(i)		
Identification and	IA-5(15)	FICAM-Approved Products and				164.308(a)(3)(ii)(B),	(a)(4)(ii), (b)(3)(i)		
Identification and	IA-6	Authenticator Feedback	X			164.308(a)(3)(ii)(B),	(a)(4)(ii), (b)(3)(i)	PR.AC-1	
Identification and	IA-7	Cryptographic Module Authentication	X			164.308(a)(3)(ii)(B),	(a)(4)(ii), (b)(3)(i)	PR.AC-1	
Identification and	IA-8	Identification and Authentication	X	X		164.308(a)(3)(ii)(B),	(a)(4)(ii), (b)(3)(i)	PR.AC-1	
Identification and	IA-8(1)	Acceptance of PIV Credentials							
Identification and	IA-8(2)	Acceptance of Third-Party Credentials	X	X					
Identification and	IA-8(3)	Use of FICAM-Approved Products							
Identification and	IA-8(4)	Use of FICAM-Issued Profiles							
Identification and	IA-9	Service Identification and						PR.AC-1	
Identification and	IA-10	Adaptive Identification and			CSC-6, CSC-16			PR.AC-1	
Identification and	IA-11	Re-Authentication						PR.AC-1	
Incident Response	IR-1	Incident Response Policy and	X			164.306,	(a)(3)(viii), (b)(3)(i),	ID.GV-1	3 years
Incident Response	IR-2	Incident Response Training	X		CSC-19	164.308(a)(6)(i);	(a)(3)(viii), (b)(3)(i)	PR.AT-5	365 days/Annually
Incident Response	IR-3	Incident Response Testing	X		CSC-19	164.308(a)(2),	(a)(3)(viii), (b)(3)(i)	PR.IP-10	365 days/Annually
Incident Response	IR-3(2)	Coordination with Related Plans	X			164.308(a)(2),	(a)(3)(viii), (b)(3)(i)		
Incident Response	IR-4	Incident Handling	X		CSC-19	164.308(a)(1)(i),	(a)(3)(viii), (b)(3)(i)	DE.AE-2	
Incident Response	IR-4(1)	Automated Incident Handling	X			164.308(a)(1)(i),	(a)(3)(viii), (b)(3)(i)		
Incident Response	IR-5	Incident Monitoring	X	X	CSC-19	164.308(a)(1)(i),	(a)(3)(viii), (b)(3)(i)	DE.AE-3	Continuous and ongoing
Incident Response	IR-6	Incident Reporting	X	X	CSC-19	164.308(a)(1)(i),	(a)(3)(viii), (b)(3)(i)	ID.SC-5	
Incident Response	IR-6(1)	Automated Reporting	X				(a)(3)(viii), (b)(3)(i)		Continuous and ongoing
Incident Response	IR-7	Incident Response Assistance	X		CSC-19	164.308(a)(6)(i)	(a)(3)(viii), (b)(3)(i)	PR.IP-9	
Incident Response	IR-7(1)	Automation Support for Availability	X				(a)(3)(viii), (b)(3)(i)		
Incident Response	IR-7(2)	Coordination with External Providers							
Incident Response	IR-8	Incident Response Plan	X	X	CSC-19	164.306(e),	(a)(3)(viii), (b)(3)(i)	DE.AE-3	
Incident Response	IR-9	Information Spillage Response	X	X	CSC-13		(a)(3)(viii), (b)(3)(i)	PR.IP-9	
Incident Response	IR-9(1)	Responsible Personnel							
Incident Response	IR-9(2)	Training							
Incident Response	IR-9(3)	Post-Spill Operations							
Incident Response	IR-9(4)	Exposure to Unauthorized Personnel							
Incident Response	IR-10	Integrated Information Security			CSC-19				
Maintenance (MA)	MA-1	System Maintenance Policy and	X			164.306,	(b)(3)(iii)	ID.GV-1	3 years
Maintenance (MA)	MA-2	Controlled Maintenance	X			164.308(a)(3)(ii)(A);		PR-MA-1	
Maintenance (MA)	MA-3	Maintenance Tools	X			164.308(a)(3)(ii)(A),		PR-MA-1	
Maintenance (MA)	MA-3(1)	Inspect Tools	X			164.308(a)(3)(ii)(A),			
Maintenance (MA)	MA-3(2)	Inspect Media	X			164.308(a)(3)(ii)(A),			
Maintenance (MA)	MA-3(3)	Prevent Unauthorized Removal	X			164.308(a)(3)(ii)(A),			
Maintenance (MA)	MA-4	Nonlocal Maintenance	X		CSC-5, CSC-7, CSC-11	164.308(a)(3)(ii)(A),		PR-MA-2	
Maintenance (MA)	MA-4(1)	Auditing and Review	X			164.308(a)(3)(ii)(A),			
Maintenance (MA)	MA-4(2)	Document Nonlocal Maintenance	X			164.308(a)(3)(ii)(A),			
Maintenance (MA)	MA-4(3)	Comparable Security/Sanitization				164.308(a)(3)(ii)(A),			
Maintenance (MA)	MA-5	Maintenance Personnel	X			164.308(a)(3)(ii)(A);		PR-MA-1	
Maintenance (MA)	MA-5(1)	Individuals Without Appropriate							
Maintenance (MA)	MA-6	Timely Maintenance	X					PR-MA-1	
Media Protection	MP-1	Media Protection Policy and	X			164.306,	(a)(4)(vi), (b)(3)(i),	ID.GV-1	3 years
Media Protection	MP-2	Media Access	X			164.308(a)(3)(i),	(a)(4)(vi), (b)(3)(i)	PR.PT-2	
Media Protection	MP-3	Media Marking	X		CSC-14	164.310(c);	(a)(4)(vi), (b)(3)(i)	PR.PT-2	
Media Protection	MP-4	Media Storage	X	X	CSC-10	164.308(a)(3)(i),	(a)(4)(vi), (b)(3)(i)	PR.PT-2	
Media Protection	MP-5	Media Transport	X		CSC-13	164.308(a)(3)(i),	(a)(4)(vi), (b)(3)(i)	PR.PT-2	
Media Protection	MP-5(4)	Cryptographic Protection	X	X		164.308(a)(3)(i),	(a)(4)(vi), (b)(3)(i)		
Media Protection	MP-6	Media Sanitization	X	X		164.308(a)(1)(ii)(A),	(a)(4)(vi), (b)(3)(i)	PR.DS-3	
Media Protection	MP-6(1)	Review/Approve/Track/Document/Ve				164.308(a)(1)(ii)(A),	(a)(4)(vi), (b)(3)(i)		

Media Protection	MP-6(2)	Equipment Testing – Enhancement				164.308(a)(1)(ii)(A),	(a)(4)(vi), (b)(3)(i)		
Media Protection	MP-7	Media Use	X			164.308(a)(3)(i),	(a)(4)(vi), (b)(3)(i)	PR.PT-2	
Media Protection	MP-7(1)	Prohibit Use Without Owner	X				(a)(4)(vi), (b)(3)(i)		
Media Protection	MP-8	Media Downgrading						PR.DS-1	
Physical and	PE-1	Physical and Environmental	X			164.306,	(b)(3)(iii)	ID.GV-1	3 years
Physical and	PE-2	Physical Access Authorizations	X			164.308(a)(1)(ii)(B),		PR.AC-2	6 months
Physical and	PE-2(1)	Access by Position / Role	X			164.308(a)(1)(ii)(B),			
Physical and	PE-3	Physical Access Control	X			164.306(e),		PR.AC-2	90 days/Quarterly
Physical and	PE-4	Access Control for Transmission	X			164.308(a)(1)(ii)(B),		PR.AC-2	
Physical and	PE-5	Access Control for Output Devices	X			164.308(a)(1)(ii)(B),		PR.AC-2	
Physical and	PE-6	Monitoring Physical Access	X			164.308(a)(1)(i)		PR.AC-2	6 months
Physical and	PE-6(1)	Intrusion Alarms/Surveillance	X			164.308(a)(1)(i)			
Physical and	PE-7	Visitor Control							
Physical and	PE-8	Visitor Access Records	X			164.310(a)(2)(iii)		PR.AC-2	Every 30 days / or within one
Physical and	PE-9	Power Equipment and Cabling				164.308(a)(1)(ii)(B),		ID.BE-4	
Physical and	PE-10	Emergency Shutoff				164.308(a)(7)(i),		PR.IP-5	
Physical and	PE-11	Emergency Power				164.308(a)(7)(i),		ID.BE-4	
Physical and	PE-12	Emergency Lighting				164.308(a)(7)(i),		PR.IP-5	
Physical and	PE-13	Fire Protection				164.308(a)(7)(i),		PR.IP-5	
Physical and	PE-13(1)	Detection Devices/Systems				164.308(a)(7)(i),			
Physical and	PE-13(2)	Suppression Devices/Systems				164.308(a)(7)(i),			
Physical and	PE-13(3)	Automatic Fire Suppression				164.308(a)(7)(i),			
Physical and	PE-14	Temperature and Humidity Controls				164.308(a)(7)(i),		PR.IP-5	
Physical and	PE-14(2)	Monitoring with Alarms /							
Physical and	PE-15	Water Damage Protection				164.308(a)(7)(i),		PR.IP-5	
Physical and	PE-16	Delivery and Removal				164.308(a)(1)(ii)(A),		PR.DS-3	
Physical and	PE-17	Alternate Work Site						PR.IP-9	
Physical and	PE-18	Location of Information System				164.308(a)(3)(i);		PR.IP-5	
Physical and	PE-19	Information Leakage				164.308(a)(1)(ii)(D),		PR.DS-5	
Physical and	PE-20	Asset Monitoring and Tracking				164.308(a)(1)(ii)(D),		DE.CM-2	
Planning (PL)	PL-1	Security Planning Policy and	X			164.306,	(b)(3)(iii)	ID.GV-1	3 years
Planning (PL)	PL-2	System Security Plan	X	X		164.306(a);		DE.DP-5	365 days/Annually
Planning (PL)	PL-2(3)	Plan/Coordinate with Other	X			164.306(e),			
Planning (PL)	PL-3	System Security Plan Update							
Planning (PL)	PL-4	Rules of Behavior	X	X					365 days/Annually
Planning (PL)	PL-4(1)	Social Media and Networking	X						
Planning (PL)	PL-5	Privacy Impact Assessment		X					
Planning (PL)	PL-6	Security-Related Activity Planning							
Planning (PL)	PL-7	Security Concept of Operations							
Planning (PL)	PL-8	Information Security Architecture	X			164.308(a)(1)(i),		ID.AM-3	
Planning (PL)	PL-9	Central Management							
Personnel Security	PS-1	Personnel Security Policy and	X			164.306,	(a)(4)(v), (b)(3)(i),	PR.IP-11	3 years
Personnel Security	PS-2	Position Risk Designation	X			164.308(a)(1)(ii)(C),	(a)(4)(v), (b)(3)(i)	PR.IP-11	365 days/Annually
Personnel Security	PS-3	Personnel Screening	X			164.308(a)(1)(ii)(C),	(a)(4)(v), (b)(3)(i)	PR.DS-5	
Personnel Security	PS-3(3)	Information with Special Protection				164.308(a)(3)(ii)(B)			
Personnel Security	PS-4	Personnel Termination	X			164.308(a)(1)(ii)(C),	(a)(4)(v), (b)(3)(i)	PR.IP-11	
Personnel Security	PS-5	Personnel Transfer	X			164.308(a)(1)(ii)(C),	(a)(4)(v), (b)(3)(i)	PR.IP-11	
Personnel Security	PS-6	Access Agreements	X			164.308(a)(1)(ii)(C),	(a)(4)(v), (b)(2),	PR.DS-5	365 days/Annually
Personnel Security	PS-7	Third-Party Personnel Security	X			164.308(a)(1)(i),	(a)(4)(v), (b)(3)(i),	ID.AM-6	
Personnel Security	PS-8	Personnel Sanctions	X			164.308(a)(1)(ii)(C),	(a)(4)(v), (b)(3)(i),	PR.IP-11	
Risk Assessment	RA-1	Risk Assessment Policy and Procedure	X			164.306,	(b)(3)(iii)	ID.GV-1	3 years
Risk Assessment	RA-2	Security Categorization			CSC-14	164.308(a)(1)(i),		ID.AM-5	
Risk Assessment	RA-3	Risk Assessment	X			164.308(a)(1)(i),	(a)(3)(viii),	ID.RA-1	365 days/Annually
Risk Assessment	RA-4	Risk Assessment Update							
Risk Assessment	RA-5	Vulnerability Scanning	X	X	CSC-3, CSC-5, CSC-7	164.306(e),	(a)(3)(viii), (b)(3)(i)	ID-RA-1	30 days / or within one month
Risk Assessment	RA-5(1)	Update Tool Capability	X			164.306(e),			
Risk Assessment	RA-5(2)	Update by Frequency/Prior to New	X			164.306(e),			30 days / or within one month
Risk Assessment	RA-5(3)	Breadth/Depth of Coverage							
Risk Assessment	RA-5(5)	Privileged Access	X						2 weeks

Risk Assessment	RA-5(6)	Automated Trend Analyses							
Risk Assessment	RA-5(8)	Review Historic Audit Logs							
Risk Assessment	RA-6	Technical Surveillance			CSC-20				
System and Services	SA-1	System and Services Acquisition	X					ID.GV-1	3 years
System and Services	SA-2	Allocation of Resources	X					ID.GV-4	
System and Services	SA-3	System Development Life Cycle	X			164.308(a)(1)(i)		PR.IP-2	
System and Services	SA-4	Acquisition Process	X	X	CSC-1, CSC-2, CSC-5, CSC-7	164.308(a)(1)(i);	(b)(1), (b)(2)(ii),	DE.CM-6	
System and Services	SA-4(1)	Functional Properties of Security	X			164.308(a)(1)(i)			
System and Services	SA-4(2)	Design/Implementation Information	X			164.308(a)(1)(i)	(b)(2)(ii)		
System and Services	SA-4(8)	Continuous Monitoring Plan							
System and Services	SA-4(9)	Functions/Ports/Protocols/Services in	X			164.308(a)(1)(i)			
System and Services	SA-4(10)	Use of Approved PIV Products							
System and Services	SA-5	Information System Documentation	X			164.308(a)(1)(ii)(A),		ID.RA-1	
System and Services	SA-6	Software Usage Restrictions							
System and Services	SA-7	User-Installed Software							
System and Services	SA-8	Security Engineering Principles	X			164.308(a)(1)(i)		PR.IP-2	
System and Services	SA-9	External Information System Services	X	X	CSC-12	164.308(a)(4)(ii)(A),	(b)(2), (b)(2)(v)	ID.AM-4	
System and Services	SA-9(1)	Risk Assessments/Organizational							
System and Services	SA-9(2)	Identification of				164.308(a)(4)(ii)(A),			
System and Services	SA-9(4)	Consistent Interests of Consumers							
System and Services	SA-9(5)	Processing, Storage, and Service				164.308(a)(4)(ii)(A),			
System and Services	SA-10	Developer Configuration	X			164.308(a)(1)(i)		PR.IP-1	
System and Services	SA-10(1)	Software / Firmware Integrity							
System and Services	SA-11	Developer Security Testing and	X		CSC-17	164.308(a)(1)(i)		PR.IP-2	
System and Services	SA-11(1)	Static Code Analysis				164.308(a)(1)(i)			
System and Services	SA-11(2)	Threat and Vulnerability Analyses							
System and Services	SA-11(8)	Dynamic Code Analysis							
System and Services	SA-12	Supply Chain Protection				164.308(a)(1)(i),			
System and Services	SA-13	Trustworthiness			CSC-18			ID.BE-5	
System and Services	SA-14	Criticality Analysis				164.308(a)(1)(i),		ID.AM-5	
System and Services	SA-15	Development Process, Standards, and	X		CSC-18	164.308(a)(1)(i)		PR.IP-2	3 years
System and Services	SA-15(9)	Use of Live Data							
System and Services	SA-16	Developer-Provided Training			CSC-17, CSC-18			PR.AT-3	
System and Services	SA-17	Developer Security Architecture and	X		CSC-18	164.308(a)(1)(i)		PR.IP-2	
System and Services	SA-18	Tamper Resistance and Detection			CSC-13			DE.DP-2	
System and Services	SA-19	Component Authenticity							
System and Services	SA-20	Customized Development of Critical			CSC-18				
System and Services	SA-21	Developer Screening			CSC-18	164.308(a)(3)(ii)(B)		PR.IP-11	
System and Services	SA-22	Unsupported System Components	X						
System and	SC-1	System and Communications	X			164.306,	(b)(3)(iii)	ID.GV-1	3 years
System and	SC-2	Application Partitioning	X			164.312(a)(1)			
System and	SC-4	Information in Shared Resources	X			164.312(a)(1)	(a)(4)(ii), (b)(3)(i)		
System and	SC-5	Denial of Service Protection	X			164.308(a)(1)(ii)(A),		PR.DS-4	
System and	SC-6	Resource Availability	X					ID.AM-5	
System and	SC-7	Boundary Protection	X	X	CSC-12	164.308(a)(1)(ii)(D),		PR.DS-5	
System and	SC-7(3)	Access Points	X			164.308(a)(1)(ii)(D),			
System and	SC-7(4)	External Telecommunications	X			164.308(a)(1)(ii)(D),			365 days/Annually
System and	SC-7(5)	Deny by Default/Allow by Exception	X			164.308(a)(1)(ii)(D),			
System and	SC-7(7)	Prevent Split Tunneling for Remote	X			164.308(a)(1)(ii)(D),			
System and	SC-7(8)	Route Traffic to Authenticated Proxy	X			164.308(a)(1)(ii)(D),			
System and	SC-7(12)	Host-Based Protection	X			164.308(a)(1)(ii)(D),			
System and	SC-7(13)	Isolation of Security	X			164.308(a)(1)(ii)(D),			
System and	SC-7(18)	Fail Secure	X			164.308(a)(1)(ii)(D),			
System and	SC-8	Transmission Confidentiality and	X	X	CSC-12, CSC-13, CSC-15	164.308(a)(1)(ii)(D),	(a)(3)(vi), (a)(4)(ii),	PR.DS-2	
System and	SC-8(1)	Cryptographic or Alternate Physical	X			164.308(a)(1)(ii)(D),	(a)(3)(vi), (a)(6),		
System and	SC-8(2)	Pre/Post Transmission Handling	X			164.308(a)(1)(ii)(D),	(a)(3)(vi), (b)(3)(i)		
System and	SC-9	Transmission Confidentiality							
System and	SC-10	Network Disconnect	X						
System and	SC-11	Trusted Path						PR.DS-2	

System and	SC-12	Cryptographic Key Establishment and	X			164.312(e)(2)(ii)		PR.DS-1	
System and	SC-12(2)	Symmetric Keys	X						
System and	SC-12(3)	Asymmetric Keys							
System and	SC-13	Cryptographic Protection	X	X		164.308(a)(1)(ii)(D),		PR.DS-5	
System and	SC-14	Public Access Protections							
System and	SC-15	Collaborative Computing Device			CSC-5, CSC-7			PR.AC-3	
System and	SC-15(1)	Physical Disconnect							
System and	SC-16	Transmission of Security Attributes			CSC-14			PR.DS-6	
System and	SC-17	Public Key Infrastructure Certificates	X		CSC-1, CSC-15, CSC-16			PR.AC-1	
System and	SC-18	Mobile Code	X		CSC-2	164.308(a)(1)(ii)(D),		DE.CM-5	
System and	SC-19	Voice Over Internet Protocol	X					PR.PT-4	
System and	SC-20	Secure Name/Address Resolution	X		CSC-9			PR.PT-4	
System and	SC-21	Secure Name/Address Resolution	X		CSC-9			PR.PT-4	
System and	SC-22	Architecture and Provisioning for	X		CSC-9			PR.PT-4	
System and	SC-23	Session Authenticity	X	X	CSC-16			PR.PT-4	
System and	SC-24	Fail in Known State	X		CSC-11			PR.PT-4	
System and	SC-25	Thin Nodes						PR.PT-4	
System and	SC-26	Honeypots							
System and	SC-27	Platform-Independent Applications							
System and	SC-28	Protection of Information at Rest	X	X	CSC-13	164.308(a)(1)(ii)(D),	(a)(3)(vi), (b)(3)(i)	PR.DS-1	
System and	SC-28(1)	Cryptographic Protection				164.312(a)(2)(iv);			
System and	SC-29	Heterogeneity						PR.PT-4	
System and	SC-30	Concealment and Misdirection							
System and	SC-31	Covert Channel Analysis			CSC-13	164.308(a)(1)(ii)(D),		PR.DS-5	
System and	SC-32	Information System Partitioning						PR.PT-4	
System and	SC-33	Transmission Preparation Integrity							
System and	SC-34	Non-Modifiable Executable Programs			CSC-2, CSC-3, CSC-5, CSC-7				
System and	SC-35	Honeyclients							
System and	SC-36	Distributed Processing and Storage						PR.PT-4	
System and	SC-37	Out-of-Band Channels						PR.PT-4	
System and	SC-38	Operations Security						PR.PT-4	
System and	SC-39	Process Isolation			CSC-8, CSC-18			PR.PT-4	
System and	SC-40	Wireless Link Protection			CSC-15			PR.PT-4	
System and	SC-41	Port and I/O Device Access			CSC-9, CSC-13			PR.PT-4	
System and	SC-42	Sensor Capability and Data							
System and	SC-43	Usage Restrictions						PR.PT-4	
System and	SC-44	Detonation Chambers			CSC-8			DE.CM-5	
System and	SC-CMS-1	Electronic mail	X						
System and	SI-1	System and Information Integrity	X			164.306,	(b)(3)(iii)	ID.GV-1	3 years
System and	SI-2	Flaw Remediation	X	X	CSC-5, CSC-7	164.308(a)(1)(i),		PR.IP-12	Continous and ongoing
System and	SI-2(1)	Central Management				164.308(a)(1)(i),			
System and	SI-2(2)	Automated Flaw Remediation Status	X						
System and	SI-2(3)	Time to Remediate Flaws /	X						Continous and ongoing
System and	SI-3	Malicious Code Protection	X	X	CSC-8	164.306(e);		DE.CM-4	Continous and ongoing
System and	SI-3(1)	Central Management				164.308(a)(1)(ii)(D),			
System and	SI-3(2)	Automatic Updates	X			164.308(a)(1)(ii)(D),			
System and	SI-3(7)	Nonsignature-Based Detection							
System and	SI-4	Information System Monitoring	X	X	CSC-1, CSC-2, CSC-3, CSC-4,	164.306(e)	(a)(3)(vi), (b)(3)(i)	ID.RA-1	Continous and ongoing
System and	SI-4(1)	System-Wide Intrusion Detection	X	X		164.306(e)			
System and	SI-4(2)	Automated Tools for Real-Time				164.306(e)			
System and	SI-4(4)	Inbound and Outbound	X			164.306(e)			
System and	SI-4(5)	System-Generated Alerts	X			164.306(e)			
System and	SI-4(14)	Wireless Intrusion Detection				164.306(e)			
System and	SI-4(16)	Correlate Monitoring Information							
System and	SI-4(23)	Host-Based Devices							
System and	SI-5	Security Alerts, Advisories, and	X			164.308(a)(1)(ii)(A),		ID.RA-1	
System and	SI-6	Security Function Verification	X		CSC-20				30 days / or within one month
System and	SI-7	Software, Firmware, and Information	X		CSC-3	164.308(a)(1)(ii)(D),	(a)(3)(vi), (b)(3)(i)	PR.DS-6	
System and	SI-7(1)	Integrity Checks	X			164.308(a)(1)(ii)(D),	(a)(3)(vi), (b)(3)(i)		24 hours

System and	SI-7(7)	Integration of Detection and	X			164.308(a)(1)(ii)(D),			
System and	SI-8	Spam Protection	X		CSC-8	164.308(a)(5)(ii)(B);		DE.CM-4	
System and	SI-8(1)	Central Management							
System and	SI-8(2)	Automatic Updates	X						
System and	SI-9	Information Input Restrictions							
System and	SI-10	Information Input Validation	X		CSC-18		(a)(3)(vi), (b)(3)(i)		
System and	SI-11	Error Handling	X		CSC-18	164.308(a)(3)(i)			
System and	SI-12	Information Handling and Retention	X			44 U.S.C. §3301,	(a)(3)(vi), (b)(3)(i)	PR.IP-2	
System and	SI-13	Predictable Failure Prevention						PR.IP-2	
System and	SI-14	Non-Persistence						PR.IP-2	
System and	SI-15	Information Output Filtering			CSC-18				
System and	SI-16	Memory Protection	X		CSC-18			PR.IP-2	
System and	SI-17	Fail-Safe Procedures						PR.IP-2	
Program	PM-1	Information Security Program Plan				164.306,		ID.GV-1	
Program	PM-2	Senior Information Security Officer				164.308(a)(2);		ID.GV-2	
Program	PM-3	Information Security Resources						ID.GV-4	
Program	PM-4	Plan of Action and Milestones Process				164.308(a)(1)(ii)(B),		ID.RA-6	
Program	PM-5	Information System Inventory			CSC-1, CSC-2	164.310(d)		ID.AM-1	
Program	PM-6	Information Security Measures of			CSC-20	164.306(e),		PR.IP-7	
Program	PM-7	Enterprise Architecture				164.308(a)(1)(i)		ID.GV-4	
Program	PM-8	Critical Infrastructure Plan				164.308(a)(1)(ii)(A),		ID.RM-3	
Program	PM-9	Risk Management Strategy				164.308(a)(1),		ID.GV-4	
Program	PM-10	Security Authorization Process				164.308(a)(2)		ID.GV-4	
Program	PM-11	Mission/Business Process Definition				164.306(a);		ID.GV-4	
Program	PM-12	Insider Threat Program				164.308(a)(1)(ii)(A),		ID.RA-3	
Program	PM-13	Information Security Workforce			CSC-17	164.308(a)(2),		PR.AT-1	
Program	PM-14	Testing, Training, and Monitoring			CSC-17, CSC-20	164.306(e),		PR.IP-10	
Program	PM-15	Contacts with Security Groups and				164.308(a)(6)		ID.RA-2	
Program	PM-16	Threat Awareness Program			CSC-17	164.308(a)(1)(ii)(A),		ID.RA-2	
Authority and	AP-1	Authority to Collect	X			164.306,	(d)		
Authority and	AP-2	Purpose Specification	X				(a)(1), (a)(3)		
Accountability,	AR-1	Governance and Privacy Program	X			164.306,	(a)(3), (a)(4), (b)(1),		2 years
Accountability,	AR-2	Privacy Impact and Privacy Program	X			164.530(c)	(a)(4)(i), (a)(4)(ii),		3 years
Accountability,	AR-3	Privacy Requirements for Contractors				164.504(e)	(a)(1), (a)(2), (a)(3),		
Accountability,	AR-4	Privacy Monitoring and Auditing	X			164.530(a)(1)(ii)	(a)(3)(viii), (a)(5),		365 days/Annually
Accountability,	AR-5	Privacy Awareness and Training	X			164.530(b)(1)	(a)(3)(viii) , (c)		365 days/Annually
Accountability,	AR-6	Privacy Reporting				160.310(a);	(a)(1)(iii)(A),		
Accountability,	AR-7	Privacy-enhanced System Design and	X			164.530(c)	(a)(3)(viii)		
Accountability,	AR-8	Accounting of Disclosures	X	X		164.528	(a)(3)(ii), (a)(3)(vi),		Continuous and ongoing
Data Quality and	DI-1	Data Quality	X			164.306,	(a)(3)(vi), (a)(4)(i),		365 days/Annually
Data Quality and	DI-1(1)	Validate PII	X			164.306,	(a)(3)(vi), (a)(4)(i)		
Data Quality and	DI-1(2)	Re-validate PII				164.306,	(a)(3)(vi), (a)(4)(i),		
Data Quality and	DI-2	Data Integrity and Data Integrity					(a)(4)(i), (e)(4)		
Data Quality and	DI-2(1)	Publish Agreements on Website					(e), (e)(4)		
Data Minimization	DM-1	Minimization of Personally	X			164.306,	(a)(1)(i), (a)(1)(ii),		365 days/Annually
Data Minimization	DM-1(1)	Minimization of	X			164.306,	(a)(1)(i), (a)(1)(ii),		
Data Minimization	DM-2	Data Retention and Disposal	X			164.310(d)(2)(i);	(a)(4)(vi)		
Data Minimization	DM-2 (1)	Data Retention and Disposal/System	X			164.310(d)(2)(i);	(a)(4)(vi)		
Data Minimization	DM-3	Minimization of PII Used in Testing,	X			164.501;	(a)(1), (a)(4)(i),		
Data Minimization	DM-3 (1)	Minimization of PII Used in Testing,	X			164.501;	(a)(1)(i), (a)(1)(ii),		
Individual	IP-1	Consent	X			164.306,	(a)(3)(iii), (a)(3)(iv),		
Individual	IP-1(1)	Mechanism Supporting Itemized or				164.306,	(a)(3)(iii), (a)(3)(iv),		
Individual	IP-2	Individual Access	X			164.524	(a)(3)(i), (a)(3)(ii),		
Individual	IP-3	Redress	X			164.526	(a)(3)(ii)		
Individual	IP-4	Complaint Management	X			164.530(d)	(a)(3)(ii)		
Individual	IP-4(1)	Complaint Management/Response	X			164.520(b)(1)(vi)	(a)(3)(ii)		
Security (SE)	SE-1	Inventory of Personally Identifiable	X	X		164.306,	(a)(3)(vii), (a)(4)(i),		Continuous and Ongoing
Security (SE)	SE-2	Privacy Incident Response	X			45 C.F.R. Part 164	(a)(3)(viii)		365 days/Annually
Transparency (TR)	TR-1	Privacy Notice	X			164.306,	(a)(3)(iii), (a)(3)(iv)		365 days/Annually

Transparency (TR)	TR-1(1)	Real-time or Layered Notice				164.306,	(a)(3)(iii), (a)(3)(iv)		
Transparency (TR)	TR-2	System of Records Notices and					(a)(3)(iii), (a)(3)(iv)		
Transparency (TR)	TR-2(1)	Public Website Publication					(a)(3)(iii), (a)(3)(iv)		
Transparency (TR)	TR-3	Dissemination of Privacy Program	X				(a)(3)(i), (a)(3)(ii),		
Use Limitation (UL)	UL-1	Internal Use	X			164.306,	(a)(1)(i),		
Use Limitation (UL)	UL-2	Information Sharing with Third	X	XK12:K475		164.502(e)(1);	(a)(4)(ii), (b)(2),		365 days/Annually