NIST Control ID	NIST Control Name	ISO 27001/2:2013	2016 SISM	FedRAMP	HIPAA Security Rule 45 C.F.R.	COBIT 5	CIS Critical Security Controls v6.1: 2016	FERPA Privacy Technical Assistance Center (PTAC) Data Security Checklist
Access Control (AC)								
AC-1	**Access Control Policy and Procedures**	A.5.1.1, A.5.1.2, A.6.1.1, A.6.2.1, A.6.2.2, A.9.1.1, A.9.1.2, A.9.2.1, A.12.1.1, A.13.2.1, A.18.1.1, A.18.2.2	020101	AC-1 (b) (1) AC-1 (b) (2)			#12: Controlled Use of Administrative Privileges #6: Maintenance, Monitoring, and Analysis of Audit Logs #14: Controlled Access Based on the Need to Know #16: Account Monitoring and Control	
AC-2	**Account Management**	A.6.1.2, A.9.1.2, A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.5, A.9.2.6, A.9.3.1, A.9.4.1, A.9.4.2, A.9.4.3, A.9.4.4, A.12.4.1, A.18.2.2	020101, 020102, 040503	AC-2 (j)	§§164.308(a)(1)(ii)(D) 164.308(a)(3), 164.308(a)(3)(ii)(A), 164.308(a)(3)(ii)(B), 164.308(a)(3)(ii)(C), 164.308(a)(4), 164.308(a)(4)(i), 164.308(a)(4)(ii)(B), 164.308(a)(4)(ii)(C), 164.308(a)(5)(ii)(B), n164.308(a)(5)(ii)(C), 164.308(a)(8), 164.310(a)(2)(iii), 164.310(b), 164.312(a)(1), 164.312(a)(2)(i), 164.312(a)(2)(ii), 64.312(a)(2)(iii), 164.312(b), 164.312(d), 164.312(e)(2)(i)	DSS05.04, DSS05.07, DSS06.03	#1: Inventory of Authorized and Unauthorized Devices #5: Controlled Use of Administrative Privileges #6: Maintenance, Monitoring, and Analysis of Audit Logs #11: Secure Configurations for Network Devices #12: Controlled Use of Administrative Privileges #14: Controlled Access Based on the Need to Know #15: Wireless Access Control #16: Account Monitoring and Control	
AC-3	**Access Enforcement**	A.6.2.2, A.9.1.2, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.1, A.13.2.1, A.14.1.2, A.14.1.3, A.18.1.3	020106		§§164.308(a)(3), 164.308(a)(4), 164.310(a)(2)(iii), 164.310(b), 164.310(c), 164.312(a)(1), 164.312(a)(2)(i), 164.312(a)(2)(ii), 164.312(a)(2)(iv)	DSS05.02	#1: Inventory of Authorized and Unauthorized Devices #6: Maintenance, Monitoring, and Analysis of Audit Logs #11: Secure Configurations for Network Devices #12: Controlled Use of Administrative Privileges #5: Controlled Use of Administrative Privileges #13: Data Protection #14: Controlled Access Based on the Need to Know #16: Account Monitoring and Control	Access control - Secure data access through strong passwords and multiple levels of user authentication, setting limits on the length of data access (e.g. , locking access after the session timeout), limiting logical access to sensitive data and resources, and limiting administrative privileges.
AC-4	**Information Flow Enforcement**	A.6.2.2, A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3	030105, 030304, 030307		§§164.308(a)(1)(ii)(A) 164.308(a)(1)(ii)(D), 164.308(a)(3), 164.308(a)(3)(ii)(A), 164.308(a)(4), 164.308(a)(4)(ii)(B), 164.308(a)(8), 164.310(a)(1), 164.310(b), 164.310(c), 164.310(d), 164.312(a), 164.312(a)(1), 164.312(b),	DSS03.01, DSS05.02, APO13.01	#5: Controlled Use of Administrative Privileges #9: Limitation and Control of Network Ports #11: Secure Configurations for Network Devices #12: Boundary Defense #13: Data Protection #19: Secure Network Engineering	

NIST Control ID	NIST Control Name	ISO 27001/2:2013	2016 SISM	FedRAMP	HIPAA Security Rule 45 C.F.R.	COBIT 5	CIS Critical Security Controls v6.1: 2016	FERPA Privacy Technical Assistance Center (PTAC) Data Security Checklist
AC-5	**Separation of Duties**	A.6.1.1, A.6.1.2, A.9.1.1, A.9.1.2, A.12.1.3	040406, 060102		§§164.308(a)(1)(ii)(D) 164.308(a)(3), 164.308(a)(4), 164.310(a)(2)(iii), 164.310(b), 164.310(c), 164.312(a), 164.312(a)(1), 164.312(a)(2)(i), 164.312(a)(2)(ii),	APO01.06		
AC-6	**Least Privilege**	A.6.1.1, A.9.1.1, A.9.1.2, A.9.2.1, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5	020101, 041205		§§164.308(a)(1)(ii)(D) 164.308(a)(3), 164.308(a)(4), 164.310(a)(2)(iii), 164.310(b), 164.310(c), 164.312(a), 164.312(a)(1), 164.312(a)(2)(i), 164.312(a)(2)(ii), 164.312e	APO01.06	#1: Inventory of Authorized and Unauthorized Devices #5: Controlled Use of Administrative Privileges #6: Maintenance, Monitoring, and Analysis of Audit Logs #9: Limitation and Control of Network Ports, Protocols and Service #11: Secure Configurations for Network Devices #14: Controlled Access Based on the Need to Know #16: Account Monitoring and Control	Role-based access - Protect PII and sensitive data-defining specified roles and privileges for user. Sensitive data that few personnel have access to should not be stored on the same server as other types of data used by more personnel without additional protections for the data (e.g., encryption).
AC-7	**Unsuccessful Logon Attempts**	A.9.4.2	020102, 020108	AC-7(a) □ AC-7(b)			#12: Controlled Use of Administrative Privileges #16: Account Monitoring and Control	
AC-8	**System Use Notification**	A.6.1.1, A.9.4.2	010203	AC-8 (a) AC-8 (c)			#12: Controlled Use of Administrative Privileges	
AC-9	**Previous Logon (Access) Notification**	A.9.4.2					#12: Controlled Use of Administrative Privileges	
AC-10	**Concurrent Session Control**	A.9.4.2	020102					
AC-11	**Session Lock**	A.9.4.2, A.11.2.8, A.11.2.9	020103, 020106, 020108				#16: Account Monitoring and Control	
AC-12	**Session Termination**		020108, 030107				#16: Account Monitoring and Control	
AC-13	**Supervision and Review**	**Withdrawn: Incorporated into AC-2 and AU-6**						
AC-14	**Permitted Actions without Identification or Authentication**	A.9.2.1, A.9.4.1	030104					
AC-15	**Automated Marking**	**Withdrawn: Incorporated into MP-3**						
AC-16	**Security Attributes**	A.6.1.2, A.7.1.2, A.8.2.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4			§§164.308(a)(3), 164.308(a)(4), 164.310(a)(2)(iii), 164.310(b), 164.312(a)(1), 164.312(a)(2)(i), 164.312(a)(2)(ii)		#1: Inventory of Authorized and Unauthorized Devices #5: Controlled Use of Administrative Privileges #11: Secure Configurations for Network Devices #12: Controlled Use of Administrative Privileges	
AC-17	**Remote Access**	A.6.2.1, A.6.2.2, A.9.1.1, A.9.1.2, A.13.1.1, A.13.2.1, A.14.1.2	020108, 030501, 030502 041003		§§164.308(a)(1)(ii)(D) 164.308(a)(4)(i), 164.308(b)(1), 164.308(b)(3), 164.310(b), 164.312(a)(1), 164.312(b), 164.312(e), 164.312(e)(1), 164.312(e)(2)(ii)	APO13.01, DSS01.04, DSS05.02, DSS05.03	#1: Inventory of Authorized and Unauthorized Devices #5: Controlled Use of Administrative Privileges #11: Secure Configurations for Network Devices #12: Boundary Defense	

NIST Control ID	NIST Control Name	ISO 27001/2:2013	2016 SISM	FedRAMP	HIPAA Security Rule 45 C.F.R.	COBIT 5	CIS Critical Security Controls v6.1: 2016	FERPA Privacy Technical Assistance Center (PTAC) Data Security Checklist
AC-18	**Wireless Access**	A.6.2.1, A.6.2.2, A.9.1.1, A.9.1.2, A.10.1.1, A.13.1.1, A.13.2.1	030501, 030701		§§164.308(a)(1)(ii)(D) 164.312(a)(1), 164.312(b), 164.312(e)		#1: Inventory of Authorized and Unauthorized Devices #5: Controlled Use of Administrative Privileges #6: Maintenance, Monitoring, and Analysis of Audit Logs #11: Secure Configurations for Network Devices #15: Wireless Access Control	
AC-19	**Access Control for Mobile Devices**	A.6.2.1, A.9.1.1, A.11.2.6, A.12.2.1, A.13.2.1	041004		§§164.308(a)(4)(i), 164.308(b)(1), 164.308(b)(3), 164.310(b), 164.312(e)(1), 164.312(e)(2)(ii)	APO13.01, DSS01.04, DSS05.03	#5: Controlled Use of Administrative Privileges #15: Wireless Access Control	Mobile devices - Encrypt sensitive data are stored on mobile devices, such as laptops or smart phones.
AC-20	**Use of External Information Systems**	A.6.1.1, A.8.1.3, A.9.1.2, A.11.2.6, A.13.1.1, A.13.2.1	020109, 041002, 041003, 041004, 041005		§§164.308(a)(4)(i), 164.308(a)(4)(ii)(A), 164.308(b), 164.308(b)(1), 164.308(b)(3), 164.310(b), 164.312(e)(1), 164.312(e)(2)(ii), 164.314(a)(1), 164.314(a)(2)(i)(B), 164.314(a)(2)(ii), 164.316(b)(2)	APO02.02	#1: Inventory of Authorized and Unauthorized Devices #11: Secure Configurations for Network Devices #12: Boundary Defense	
AC-21	**Information Sharing**	A.9.2.1	020109, 041204, 041401, 041403		§§164.308(a)(6)(ii)			
AC-22	**Publicly Accessible Content**		030104	AC-22 (d)				
AC-23	**Data Mining Protection**						#6: Maintenance, Monitoring, and Analysis of Audit Logs #13: Data Protection	
AC-24	**Access Control Decisions**	A.9.4.1					#12: Controlled Use of Administrative Privileges #14: Controlled Access Based on the Need to Know	
AC-25	**Reference Monitor**							
				Awareness & Training (AT)				
AT-1	**Security Awareness and Training Policy and Procedures**	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2	020301	AT-1 (b) (1) AT-1 (b) (2)			#17: Security Skills Assessment and Appropriate Training	Specify employee responsibilities associated with maintaining compliance with security policies
AT-2	**Security Awareness Training**	A.6.1.1, A.7.2.2, A.11.1.5, A.12.2.1	020301, 020302, 020303	AT-2(c)	§§164.308(a)(5)	APO07.03, BAI05.07	#8: Malware Defenses #17: Security Skills Assessment and Appropriate Training	Emailing confidential data - Consider the sensitivity level of the data to be sent over the email. Avoid sending unprotected PII or sensitive data by email. Organizations should use alternative practices to protect transmissions of these data. These practices include mailing paper copies via secure carrier, de-sensitizing data before transmission, and applying technical solutions for transferring files electronically (e.g., encrypting data files and/or encrypting email transmissions themselves).

NIST Control ID	NIST Control Name	ISO 27001/2:2013	2016 SISM	FedRAMP	HIPAA Security Rule 45 C.F.R.	COBIT 5	CIS Critical Security Controls v6.1: 2016	FERPA Privacy Technical Assistance Center (PTAC) Data Security Checklist
AT-3	**Role-Based Security Training**	A.6.1.1, A.7.2.2, A.11.1.5	020303	AT-3 ©	§§164.308(a)(2), 164.308(a)(3)(i), 164.308(a)(5)(i), 164.308(a)(5)(ii)(A), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(5)(ii)(D), 164.530(b)(1)	APO07.02, APO07.03, DSS06.03	#17: Security Skills Assessment and Appropriate Training	
AT-4	**Security Training Records**			AT-4 (b)			#17: Security Skills Assessment and Appropriate Training	
AT-5	**Contacts with Security Groups and Associations**	**Withdrawn: Incorporated into PM-15**						
Audit & Accountability (AU)								
AU-1	**Audit and Accountability Policy and Procedures**	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.12.1.2, A.12.4.1, A.12.7.1, A.18.1.1, A.18.2.2	040510	AU-1 (b) (1) AU-1 (b) (2)	§§164.308(a)(1)(ii)(D) 164.308(a)(5)(ii)(C), 164.310(a)(2)(iv), 164.310(d)(2)(iii), 164.312(b)			
AU-2	**Audit Events**	A.12.1.1, A.12.4.1, A.12.4.3, A.12.7.1	040510	AU-2 (a) AU-2 (d)	§§164.308(a)(1)(ii)(D) 164.308(a)(5)(ii)(C), 164.310(a)(2)(iv), 164.310(d)(2)(iii), 164.312(b)		#6: Maintenance, Monitoring, and Analysis of Audit Logs	
AU-3	**Content of Audit Records**	A.12.1.1, A.12.4.1	040510		§§164.308(a)(1)(ii)(D) 164.308(a)(5)(ii)(C), 164.310(a)(2)(iv), 164.310(d)(2)(iii), 164.312(b)		#5: Controlled Use of Administrative Privileges #6: Maintenance, Monitoring, and Analysis of Audit Logs #15: Wireless Access Control	
AU-4	**Audit Storage Capacity**	A.12.1.1, A.12.1.3, A.12.4.1	040510		§§164.308(a)(1)(ii)(D) 164.308(a)(5)(ii)(C), 164.310(a)(2)(iv), 164.310(d)(2)(iii), 164.312(b)	APO13.01	#6: Maintenance, Monitoring, and Analysis of Audit Logs	
AU-5	**Response to Audit Processing Failures**	A.12.1.1, A.12.4.1	040510	AU-5(b)	§§164.308(a)(1)(ii)(D) 164.308(a)(5)(ii)(C), 164.310(a)(2)(iv), 164.310(d)(2)(iii), 164.312(b)		#6: Maintenance, Monitoring, and Analysis of Audit Logs	

NIST Control ID	NIST Control Name	ISO 27001/2:2013	2016 SISM	FedRAMP	HIPAA Security Rule 45 C.F.R.	COBIT 5	CIS Critical Security Controls v6.1: 2016	FERPA Privacy Technical Assistance Center (PTAC) Data Security Checklist
AU-6	**Audit Review, Analysis, and Reporting**	A.12.1.2, A.12.4.1, A.16.1.2, A.16.1.4	040510	AU-6(a)-1	§§164.308(a)(1)(i), 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(6)(i), 164.308(a)(6)(ii), 164.308(a)(8), 164.310(a)(2)(iv), 164.310(d)(2)(iii), 164.312(b), 164.314(a)(2)(i)(C), 164.314(a)(2)(iii)	APO12.06, DSS02.07	#5: Controlled Use of Administrative Privileges #6: Maintenance, Monitoring, and Analysis of Audit Logs #15: Wireless Access Control #19: Incident Response and Management	
AU-7	**Audit Reduction and Report Generation**	A.12.1.2, A.16.1.7			§§164.308(a)(6)		#6: Maintenance, Monitoring, and Analysis of Audit Logs	
AU-8	**Time Stamps**	A.12.1.1, A.12.4.1, A.12.12.4	030101		§§164.308(a)(1)(ii)(D) 164.308(a)(5)(ii)(C), 164.310(a)(2)(iv), 164.310(d)(2)(iii), 164.312(b)		#6: Maintenance, Monitoring, and Analysis of Audit Logs	
AU-9	**Protection of Audit Information**	A.12.4.2, A.12.4.3, A.16.1.7, A.18.1.3	040510		§§164.308(a)(1)(ii)(D) 164.308(a)(5)(ii)(C), 164.310(a)(2)(iv), 164.310(d)(2)(iii), 164.312(b)		#6: Maintenance, Monitoring, and Analysis of Audit Logs	
AU-10	**Non-repudiation**	A.14.1.2					#6: Maintenance, Monitoring, and Analysis of Audit Logs	
AU-11	**Audit Record Retention**	A.12.1.1, A.12.4.1, A.16.1.7, A.18.1.3	040510	AU-11	§§164.308(a)(1)(ii)(D) 164.308(a)(5)(ii)(C), 164.310(a)(2)(iv), 164.310(d)(2)(iii), 164.312(b)		#5: Controlled Use of Administrative Privileges #6: Maintenance, Monitoring, and Analysis of Audit Logs #15: Wireless Access Control #19: Incident Response and Management	
AU-12	**Audit Generation**	A.12.1.1, A.12.4.1, A.12.4.3	040510	AU-12 (a)	§§164.308(a)(1)(ii)(D) 164.308(a)(3)(ii)(A), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(8), 164.310(a)(2)(iii), 164.310(a)(2)(iv), 164.310(b), 164.310(c), 164.310(d)(1), 164.310(d)(2)(iii), 164.312(a)(2)(i), 164.312(b), 164.312(d), 164.312(e), 164.312(e)(2)(i), 164.314(b)(2)(i)	DSS05.07	#5: Controlled Use of Administrative Privileges #6: Maintenance, Monitoring, and Analysis of Audit Logs #15: Wireless Access Control	

NIST Control ID	NIST Control Name	ISO 27001/2:2013	2016 SISM	FedRAMP	HIPAA Security Rule 45 C.F.R.	COBIT 5	CIS Critical Security Controls v6.1: 2016	FERPA Privacy Technical Assistance Center (PTAC) Data Security Checklist
AU-13	**Monitoring for Information Disclosure**				§§164.308(a)(1)(ii)(D) 164.308(a)(3)(ii)(A), 164.308(a)(5)(ii)(C), 164.312(a)(2)(i), 164.312(b), 164.312(d), 164.312(e)		#6: Maintenance, Monitoring, and Analysis of Audit Logs	
AU-14	**Session Audit**	A.12.4.1					#15: Wireless Access Control #5: Controlled Use of Administrative Privileges #6: Maintenance, Monitoring, and Analysis of Audit Logs	
AU-15	**Alternate Audit Capability**							
AU-16	**Cross-Organizational Auditing**	A.15.1.1, A.15.1.2						
Security Assessment & Authorization (CA)								
CA-1	**Security Assessment and Authorization Policies and Procedures**	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2		CA-1 (b)(1) CA-1 (b)(2)				
CA-2	**Security Assessments**	A.14.2.8, A.14.2.9, A.15.1.1, A.15.1.2, A.18.2.1, A.18.2.2, A.18.2.3	070202, 070203	CA-2 (b) CA-2 (d) CA-2(1)	§§164.306(e), 164.308(a)(1)(i), 164.308(a)(1)(ii)(A), 164.308(a)(2), 164.308(a)(3)(ii)(A), 164.308(a)(3)(ii)(B), 164.308(a)(4), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(7)(ii)(D), 164.308(a)(7)(ii)(E), 164.308(a)(6)(ii), 164.308(a)(8), 164.310(a)(1), 164.310(a)(2)(iii), 164.312(a)(1), 164.312(a)(2)(ii), 164.314(a)(2)(i)(C), 164.314(a)(2)(iii), 164.316(b)(2)(iii)	APO12.01, APO12.02, APO12.03, APO12.04, APO11.06, DSS04.05, DSS05.01	#3: Secure Configuration for End-User Devices #4: Continuous Vulnerability Assessment and Remediation #6: Maintenance, Monitoring, and Analysis of Audit Logs #20: Penetration Tests and Red Team Exercises	Audit and compliance monitoring - Conduct independent assessment of data protection capabilities and procedures
CA-3	**System Interconnections**	A.13.1.1, A.13.1.2, A.13.2.1, A.13.2.2, A.15.1.1, A.15.1.2	030101, 030105, 030106	CA-3 ©	§§164.308(a)(1)(ii)(A) 164.308(a)(1)(ii)(D), 164.308(a)(3)(ii)(A), 164.308(a)(8), 164.310(d), 164.312(b)	DSS03.01, DSS05.02	#9: Limitation and Control of Network Ports #11: Secure Configurations for Network Devices #12: Boundary Defense #15: Wireless Access Control	
CA-4	**Security Certification**	**Withdrawn: Incorporated into CA-2**						
CA-5	**Plan of Action and Milestones**		070202	CA-5 CA-5(b)			#20: Penetration Tests and Red Team Exercises	
CA-6	**Security Authorization**	A.14.2.9	040504	CA-6c CA-6 (c)	.		#14: Controlled Access Based on Need to Know #20: Penetration Tests and Red Team Exercises	

NIST Control ID	NIST Control Name	ISO 27001/2:2013	2016 SISM	FedRAMP	HIPAA Security Rule 45 C.F.R.	COBIT 5	CIS Critical Security Controls v6.1: 2016	FERPA Privacy Technical Assistance Center (PTAC) Data Security Checklist
CA-7	**Continuous Monitoring**	A.18.2.1, A.18.2.2, A.18.2.3	040510	CA-7 CA-7 (g)	§§164.306(e), 164.308(a)(1)(i), 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(1)(ii)(D), 164.308(a)(2), 164.308(a)(3)(ii)(A), 164.308(a)(3)(ii)(B), 164.308(a)(4), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(6)(i), 164.308(a)(6)(ii), 164.308(a)(7)(ii)(D), 164.308(a)(7)(ii)(E), 164.308(a)(8), 164.310(a)(1), 164.310(a)(2)(ii), 164.310(a)(2)(iii), 164.310(b), 164.310(c), 164.310(d)(1), 164.310(d)(2)(iii), 164.312(a)(1), 164.312(a)(2)(i), 164.312(a)(2)(ii), 164.312(b), 164.314(b)(2)(i), 164.312(d), 164.312(e), 164.312(e)(2)(i), 164.314(a)(2)(i)(C),	APO07.06, APO11.06, APO12.01, APO12.02, APO12.03, APO12.04, APO12.06, APO13.02, DSS04.05, DSS05.01, DSS05.07	#1: Inventory of Authorized and Unauthorized Devices #2: Inventory of Authorized and Unauthorized Software #3: Secure Configurations for End-User Devices #4: Continuous Vulnerability Assessment and Remediation #5: Controlled Use of Administrative Privileges #6: Maintenance, Monitoring, and Analysis of Audit Logs #7: Email and Web Browser Protections #8: Malware Defenses #9: Limitation and Control of Network Ports #11: Secure Configurations for Network Devices #12: Boundary Defense #13: Data Protection #14: Controlled Access Based on the Need to Know #15: Wireless Access Control #16: Account Monitoring and Control	
CA-8	**Penetration Testing**		060102		§§164.308(a)(1)(ii)(A), 164.308(a)(7)(ii)(E), 164.308(a)(8), 164.310(a)(1), 164.312(a)(1), 164.316(b)(2)(iii)	APO12.01, APO12.02, APO12.03, APO12.04	#20: Penetration Tests and Red Team Exercises	
CA-9	**Internal System Connections**		020104, 030101, 030102		§§164.308(a)(1)(ii)(A) 164.308(a)(3)(ii)(A), 164.308(a)(8), 164.310(d)	DSS05.02	#9: Limitation and Control of Network Ports #11: Secure Configurations for Network Devices #12: Boundary Defense #13: Data Protection	
Configuration Management (CM)								
CM-1	**Configuration Management Policy and Procedures**	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.12.5.1, A.14.2.2, A.18.1.1, A.18.2.2		CM-1 (b) (1) CM-1 (b) (2)				
CM-2	**Baseline Configuration**	A.12.1.4, A.12.5.1	040408, 040509		§§164.308(a)(1)(ii)(D), 164.308(a)(4), 164.312(b)	BAI07.04, BAI10.01, BAI10.02, BAI10.03, BAI10.05, DSS03.01	#2: Inventory of Authorized and Unauthorized Software #3: Secure Configurations for End-User Devices #7: Email and Web Browser Protections #9: Limitation and Control of Network Ports #11: Secure Configurations for Network Devices #12: Boundary Defense #15: Wireless Access Control	Network mapping - Capture network servers, routers, applications and associated data.

NIST Control ID	NIST Control Name	ISO 27001/2:2013	2016 SISM	FedRAMP	HIPAA Security Rule 45 C.F.R.	COBIT 5	CIS Critical Security Controls v6.1: 2016	FERPA Privacy Technical Assistance Center (PTAC) Data Security Checklist
CM-3	**Configuration Change Control**	A.12.1.2, A.12.5.1, A.14.2.2, A.14.2.3, A.14.2.4, A.14.2.9	040402, 040405,		§§164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(8), 164.310(a)(1), 164.310(a)(2)(ii), 164.310(a)(2)(iii), 164.310(b), 164.310(c), 164.310(d)(1), 164.310(d)(2)(iii), 164.312(b), 164.314(b)(2)(i), 164.312(e)(2)(i),	BAI01.06, BAI06.01, BAI10.01, BAI10.02, BAI10.03, BAI10.05, DSS05.07	#3: Secure Configuration for End-User Devices #7: Email and Web Browser Protections #11: Secure Configurations for Network Devices	Change management - Analyze and address security and privacy risks introduced by new technology or business processes.
CM-4	**Security Impact Analysis**	A.12.5.1, A.14.2.3, A.14.2.4, A.14.2.9	070102		§§164.308(a)(4), 164.308(a)(8), 164.308(a)(7)(i), 164.308(a)(7)(ii)	BAI01.06, BAI06.01, BAI10.01, BAI10.02, BAI10.03, BAI10.05		
CM-5	**Access Restrictions for Change**	A.9.1.1, A.9.2.1, A.9.2.3, A.9.4.1, A.9.4.5, A.12.1.2, A.12.1.4, A.12.5.1, A.14.2.4	040301, 040302, 040405		§§164.308(a)(8), 164.308(a)(7)(i), 164.308(a)(7)(ii)	BAI10.01, BAI10.02, BAI10.03, BAI10.05	#2: Inventory of Authorized and Unauthorized Software #3: Secure Configuration for End-User Devices #6: Maintenance, Monitoring, and Analysis of Audit Logs #7: Email and Web Browser Protections #11: Secure Configurations for Network Devices #12: Controlled Use of Administrative Privileges	
CM-6	**Configuration Settings**		030103, 030601, 040408, 040906	CM-6 (a)	§§164.308(a)(8), 164.308(a)(7)(i), 164.308(a)(7)(ii)	BAI10.01, BAI10.02, BAI10.03, BAI10.05	#3: Secure Configuration for End-User Devices #7: Email and Web Browser Protections #9: Limitation and Control of Network Ports #11: Secure Configurations for Network Devices	Secure configurations - Security test hardware and software configurations to optimize its security.
CM-7	**Least Functionality**	A.12.5.1	020101, 030302, 030601, 040701, 040906	CM-7 CM-7 (b)	§§164.308(a)(3), 164.308(a)(4), 164.308(a)(8), 164.308(a)(7)(i), 164.308(a)(7)(ii), 164.310(a)(2)(iii), 164.310(b), 164.310(c), 164.312(a)(1), 164.312(a)(2)(i), 164.312(a)(2)(ii), 164.312(a)(2)(iv)	BAI10.01, BAI10.02, BAI10.03, BAI10.05, DSS05.02	#2: Inventory of Authorized and Unauthorized Software #3: Secure Configuration for End-User Devices #7: Email and Web Browser Protections	

NIST Control ID	NIST Control Name	ISO 27001/2:2013	2016 SISM	FedRAMP	HIPAA Security Rule 45 C.F.R.	COBIT 5	CIS Critical Security Controls v6.1: 2016	FERPA Privacy Technical Assistance Center (PTAC) Data Security Checklist
CM-8	**Information System Component Inventory**	A.8.1.1, A.8.1.2	040407, 041101	CM-8 CM-8 (b)	§§164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(D), 164.308(a)(3)(ii)(A), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(7)(ii)(E), 164.308(a)(8), 164.310(a)(1), 164.310(a)(2)(ii), 164.310(a)(2)(iii), 164.310(a)(2)(iv), 164.310(b), 164.310(c), 164.310(d), 164.310(d)(1), 164.310(d)(2), 164.310(d)(2)(iii), 164.312(b), 164.314(b)(2)(i)	BAI09.01, BAI09.02, BAI09.03, BAI09.05	#1: Inventory of Authorized and Unauthorized Devices #2: Inventory of Authorized and Unauthorized Software #3: Secure Configuration for End-User Devices #7: Email and Web Browser Protections #9: Limitation and Control of Network Ports #11: Secure Configurations for Network Devices	Inventory of assets - Include both authorized and unauthorized devices used in the computing environment.
CM-9	**Configuration Management Plan**	A.6.1.1, A.8.1.1, A.8.1.2, A.9.4.5, A.12.5.1, A.14.2.2, A.14.2.3, A.14.2.4, A.14.2.9	040102, 040203, 040406, 040509		§§164.308(a)(8), 164.308(a)(7)(i), 164.308(a)(7)(ii)	BAI10.01, BAI10.02, BAI10.03, BAI10.05	#3: Secure Configuration for End-User Devices #7: Email and Web Browser Protections	
CM-10	**Software Usage Restrictions**	A.12.5.1, A.18.1.2, A.14.2.7	010202, 040101		§§164.308(a)(1)(ii)(D), 164.308(a)(3)(ii)(A), 164.308(a)(5)(ii)(C), 164.312(a)(2)(i), 164.312(b), 164.312(d), 164.312(e)		#2: Inventory of Authorized and Unauthorized Software	
CM-11	**User-Installed Software**	A.12.5.1, A.12.6.2, A.14.2.7	020201, 040102	CM-11	§§164.308(a)(1)(ii)(D), 164.308(a)(3)(ii)(A), 164.308(a)(5)(ii)(C), 164.312(a)(2)(i), 164.312(b), 164.312(d),		#2: Inventory of Authorized and Unauthorized Software #3: Secure Configuration for End-User Devices #7: Email and Web Browser Protections	
Contingency Planning (CP)								
CP-1	**Contingency Planning Policy and Procedures**	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.17.1.1, A.18.1.1, A.18.2.2	070101, 070102,	CP-1 (b)(1) CP-1 (b)(2)				

NIST Control ID	NIST Control Name	ISO 27001/2:2013	2016 SISM	FedRAMP	HIPAA Security Rule 45 C.F.R.	COBIT 5	CIS Critical Security Controls v6.1: 2016	FERPA Privacy Technical Assistance Center (PTAC) Data Security Checklist
CP-2	**Contingency Plan**	A.6.1.1, A.11.1.4, A.17.1.1, A.17.1.3, A.17.2.1	070103	CP-2 CP-2 (d)	§§164.306(e), 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(2), 164.308(a)(3), 164.308(a)(4), 164.308(a)(4)(ii), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(6), 164.308(a)(6)(i), 164.308(a)(6)(ii), 164.308(a)(7), 164.308(a)(7)(i), 164.308(a)(7)(ii)(A), 164.308(a)(7)(ii)(B), 164.308(a)(7)(ii)(C), 164.308(a)(7)(ii)(D), 164.308(a)(7)(ii)(E), 164.308(a)(8), 164.308(b)(1), 164.310(a)(2)(i), 164.310(d)(2)(iv), 164.312(a)(2)(ii), 164.314, 164.314(a)(2)(i)(C), 164.314(b)(2)(i), 164.316, 164.316(b)(2)(iii)	APO01.02, APO03.03, APO03.04, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05, APO11.06, APO12.06, APO13.01, BAI01.10, BAI01.13, BAI05.07, BAI09.02, DSS02.05, DSS03.04, DSS04.02, DSS04.03, DSS04.05, DSS06.03		
CP-3	**Contingency Training**	A.7.2.2, A.11.1.4	070103	CP-3 (a) CP-3 (c)	§§164.308(a)(2), 164.308(a)(6)(i), 164.308(a)(7)(ii)(A), 164.308(a)(7)(ii)(B), 164.308(a)(7)(ii)(C), 164.310(a)(2)(i), 164.312(a)(2)(ii)		#17: Security Skills Assessment and Appropriate Training	
CP-4	**Contingency Plan Testing**	A.11.1.4, A.17.1.1, A.17.1.3	070103, 070104	CP-4(a) CP-4 (a)-1 CP-4 (a)-2	§§164.308(a)(7)(ii)(A) 164.308(a)(7)(ii)(B), 164.308(a)(7)(ii)(D), 164.310(a)(2)(i), 164.310(d)(2)(iv)	APO13.01		
CP-5	**Contingency Plan Update**	**Withdrawn: Incorporated into CP-2**						
CP-6	**Alternate Storage Site**	A.11.1.4, A.17.1.2, A.17.2.1	050202		§§164.308(a)(7)(ii)(A) 164.308(a)(7)(ii)(B), 164.308(a)(7)(ii)(D), 164.310(a)(2)(i), 164.310(d)(2)(iv)	APO13.01		
CP-7	**Alternate Processing Site**	A.11.1.4, A.17.1.2, A.17.2.1						
CP-8	**Telecommunications Services**	A.11.1.4, A.11.2.2, A.13.1.1, A.17.1.2	030103		§§164.308(a)(1)(ii)(D), 164.308(a)(7)(i), 164.308.(a)(7)(ii)(E), 164.310(a)(2)(i), 164.312(a)(1), 164.312(a)(2)(ii), 164.312(b), 164.312€, 164.314(a)(1), 164.314(b)(2)(i)	DSS05.02, APO13.01		

NIST Control ID	NIST Control Name	ISO 27001/2:2013	2016 SISM	FedRAMP	HIPAA Security Rule 45 C.F.R.	COBIT 5	CIS Critical Security Controls v6.1: 2016	FERPA Privacy Technical Assistance Center (PTAC) Data Security Checklist
CP-9	**Information System Backup**	A.11.1.4, A.12.3.1, A.17.1.2, A.18.1.3	041301, 041302,	CP-9 CP-9 (a) CP-9 (b) CP-9 (c)	§§164.308(a)(7)(ii)(A), 164.308(a)(7)(ii)(B), 164.308(a)(7)(ii)(D), 164.310(a)(2)(i), 164.310(d)(2)(iv)	APO13.01	#10: Data Recovery Capability #13: Data Protection	
CP-10	**Information System Recovery and Reconstitution**	A.11.1.4, A.17.1.2	070104		§§164.308(a)(6)(ii), 164.308(a)(7), 164.308(a)(7)(i), 164.308(a)(7)(ii)(A), 164.308(a)(7)(ii)(B), 164.308(a)(7)(ii)(C), 164.310(a)(2)(i), 164.312(a)(2)(ii)	BAI01.10, DSS02.05, DSS03.04	#10 Data Recovery Capability	
CP-11	**Alternate Communications Protocols**	A.11.1.4, A.17.1.2			§§164.308(a)(1)(ii)(B), 164.308(a)(6)(ii), 164.308(a)(7), 164.308(a)(8), 164.310(a)(2)(i), 164.312(a)(2)(ii), 164.314(b)(2)(i)	DSS04.0		
CP-12	**Safe Mode**	A.11.1.4						
CP-13	**Alternative Security Mechanisms**	A.11.1.4, A.17.1.2						
				Identification & Authentication (IA)				
IA-1	**Identification and Authentication Policy and Procedures**	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2	020102	IA-1 (b) (1) IA-1 (b) (2)	§§164.308(a)(3)(ii)(B), 164.308(a)(3)(ii)(C), 164.308(a)(4)(i), 164.308(a)(4)(ii)(B), 164.308(a)(4)(ii)(C), 164.312(a)(2)(i), 164.312(a)(2)(ii), 64.312(a)(2)(iii), 164.312(d)			
IA-2	**Identification and Authentication (Organizational Users)**	A.9.2.1, A.9.3.1, A.9.4.2, A.9.4.3, A.11.2.8	020101, 020102, 020108	IA-2 (12)	§§164.308(a)(3)(ii)(B), 164.308(a)(3)(ii)(C), 164.308(a)(4)(i), 164.308(a)(4)(ii)(B), 164.308(a)(4)(ii)(C), 164.312(a)(2)(i), 164.312(a)(2)(ii), 64.312(a)(2)(iii), 164.312(d)		#5: Controlled Use of Administrative Privileges	Authentication - Consider TFA for remote users or privileged “super users.”
IA-3	**Device Identification and Authentication**		030108				#1: Inventory of Authorized and Unauthorized Devices #15: Wireless Access Control	
IA-4	**Identifier Management**	A.9.2.1, A.16.1.6, A.16.1.7	020102, 020108	IA-4 (d) IA-4 (e)	§§164.308(a)(3)(ii)(B), 164.308(a)(3)(ii)(C), 164.308(a)(4)(i), 164.308(a)(4)(ii)(B), 164.308(a)(4)(ii)(C), 164.308(a)(6)(i), 164.312(a)(2)(i), 164.312(a)(2)(ii), 64.312(a)(2)(iii), 164.312(d)		#5: Controlled Use of Administrative Privileges	

NIST Control ID	NIST Control Name	ISO 27001/2:2013	2016 SISM	FedRAMP	HIPAA Security Rule 45 C.F.R.	COBIT 5	CIS Critical Security Controls v6.1: 2016	FERPA Privacy Technical Assistance Center (PTAC) Data Security Checklist
IA-5	**Authenticator Management**	A.9.2.1, A.9.2.3, A.9.2.4, A.9.3.1, A.9.4.3	020106	IA-5 (1) (a) IA-5 (1) (b) IA-5 (1) (d) IA-5 (1) (e) IA-5 (g)	§§164.308(a)(3)(ii)(B), 164.308(a)(3)(ii)(C), 164.308(a)(4)(i), 164.308(a)(4)(ii)(B), 164.308(a)(4)(ii)(C), 164.308(a)(6)(i), 164.312(a)(2)(i), 164.312(a)(2)(ii), 64.312(a)(2)(iii), 164.312(d)		#5: Controlled Use of Administrative Privileges #12: Controlled Use of Administrative Privileges #16: Account Monitoring and Control	
IA-6	**Authenticator Feedback**	A.9.4.2	020106		§§164.308(a)(3)(ii)(B), 164.308(a)(3)(ii)(C), 164.308(a)(4)(i), 164.308(a)(4)(ii)(B), 164.308(a)(4)(ii)(C), 164.312(a)(2)(i), 164.312(a)(2)(ii), 64.312(a)(2)(iii), 164.312(d)		#12: Controlled Use of Administrative Privileges #16: Account Monitoring and Control	
IA-7	**Cryptographic Module Authentication**	A.10.1.1, A.18.1.1, A.18.1.5, A.18.2.2			§§164.308(a)(3)(ii)(B), 164.308(a)(3)(ii)(C), 164.308(a)(4)(i), 164.308(a)(4)(ii)(B), 164.308(a)(4)(ii)(C), 164.312(a)(2)(i), 164.312(a)(2)(ii), 64.312(a)(2)(iii), 164.312(d)		#13: Data Protection	
IA-8	**Identification and Authentication (Non-Organizational Users)**	A.9.2.1, A.9.4.2, A.14.1.2	020101, 020102, 020108		§§164.308(a)(3)(ii)(B), 164.308(a)(3)(ii)(C), 164.308(a)(4)(i), 164.308(a)(4)(ii)(B), 164.308(a)(4)(ii)(C), 164.308(a)(6)(i), 164.312(a)(2)(i), 164.312(a)(2)(ii), 64.312(a)(2)(iii), 164.312(d)			
IA-9	**Service Identification and Authentication**							
IA-10	**Adaptive Identification and Authentication**						#6: Maintenance, Monitoring, and Analysis of Audit Logs #16: Account Monitoring and Control	
IA-11	**Re-authentication**		020108, 030107					
Incident Response (IR)								
IR-1	**Incident Response Policy and Procedures**	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.16.1.1, A.16.1.2, A.18.1.1, A.18.2.2	060101	IR-1 (b) (1) IR-1 (b) (2)			#19: Incident Response and Management	
IR-2	**Incident Response Training**	A.7.2.2	020303, 070103	IR-2 (c)			#17: Security Skills Assessment and Appropriate Training #19: Incident Response and Management	

NIST Control ID	NIST Control Name	ISO 27001/2:2013	2016 SISM	FedRAMP	HIPAA Security Rule 45 C.F.R.	COBIT 5	CIS Critical Security Controls v6.1: 2016	FERPA Privacy Technical Assistance Center (PTAC) Data Security Checklist
IR-3	**Incident Response Testing**		060101, 070103		§§164.308(a)(2), 164.308(a)(7)(ii)(A), 164.308(a)(7)(ii)(B), 164.308(a)(7)(ii)(C), 164.308(a)(7)(ii)(D),164.310(a)(2)(i), 164.308(a)(6)(i), 164.312(a)(2)(ii)		#19: Incident Response and Management	
IR-4	**Incident Handling**	A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7	060203	IR-4	§§164.308(a)(1)(i), 164.308(a)(1)(ii)(B), 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(6), 164.308(a)(6)(i), 164.308(a)(6)(ii), 164.308(a)(7), 164.308(a)(7)(i), 164.308(a)(7)(ii)(A), 164.308(a)(7)(ii)(B), 164.308(a)(7)(ii)(C), 164.308(a)(7)(ii)(D), 164.308(a)(7)(ii)(E), 164.308(a)(8), 164.310(a)(2)(i), 164.310(d)(2)(iii), 164.312(a)(2)(ii), 164.312(b), 164.314(a)(2)(i)(C), 164.314(a)(2)(iii), 164.316(b)(2)(iii)	APO12.06, BAI01.10, BAI01.13, BAI05.07, BAI07.08, DSS02.05, DSS02.07, DSS03.04	#19: Incident Response and Management	Incident handling - Establish procedures for users, security personnel, and managers need to be established to define the appropriate roles and actions. Outside experts may be required to conduct forensic investigations.
IR-5	**Incident Monitoring**		060203		§§164.308(a)(1)(i), 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(6)(ii), 164.312(b)	APO12.06	#19: Incident Response and Management	
IR-6	**Incident Reporting**	A.6.1.3, A.16.1.2	060201, 060202	IR-6 (a)	§§164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(6)(ii), 164.314(a)(2)(i)(C), 164.314(a)(2)(iii)		#19: Incident Response and Management	
IR-7	**Incident Response Assistance**		060203				#19: Incident Response and Management	

NIST Control ID	NIST Control Name	ISO 27001/2:2013	2016 SISM	FedRAMP	HIPAA Security Rule 45 C.F.R.	COBIT 5	CIS Critical Security Controls v6.1: 2016	FERPA Privacy Technical Assistance Center (PTAC) Data Security Checklist
IR-8	**Incident Response Plan**	A.16.1.1	060101	IR-8 (b) IR-8 (c) IR-8 (e)	§§164.306(e), 164.308(a)(2), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(6), 164.308(a)(6)(i), 164.308(a)(6)(ii), 164.308(a)(7), 164.308(a)(7)(i), 164.308(a)(7)(ii)(A), 164.308(a)(7)(ii)(B), 164.308(a)(7)(ii)(C), 164.308(a)(7)(ii)(D), 164.308(a)(8), 164.310(a)(2)(i), 164.312(a)(2)(ii), 164.314(a)(2)(i)(C), 164.314(a)(2)(iii), 164.316(b)(2)(iii)	COBIT 5 APO12.06, BAI01.13, BAI05.07, BAI07.08, DSS02.05, DSS03.04, DSS04.03	#19: Incident Response and Management	
IR-9	**Information Spillage Response**		060204				#13: Data Protection	
IR-10	**Integrated Information Security Analysis Team**						#19: Incident Response and Management	
Maintenance (MA)								
MA-1	**System Maintenance Policy and Procedures**	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2	040509	MA-1 (b) (1) MA-1 (b) (2)				
MA-2	**Controlled Maintenance**	A.11.2.4, A.11.2.5	040102, 040202, 40203, 040205, 040303, 040405, 040509		§§164.308(a)(3)(ii)(A) 164.310(a)(2)(iv)	BAI09.03		
MA-3	**Maintenance Tools**	A.11.2.4	020104, 040102		§§164.308(a)(3)(ii)(A) 164.310(a)(2)(iv)	BAI09.03		
MA-4	**Nonlocal Maintenance**	A.11.2.4	020108		§§164.308(a)(3)(ii)(A) 164.310(d)(1), 164.310(d)(2)(ii), 164.310(d)(2)(iii), 164.312(a), 164.312(a)(2)(ii), 164.312(a)(2)(iv), 164.312(b), 164.312(d), 164.312(e), 164.308(a)(1)(ii)(D)	DSS05.04	#3: Secure Configuration for End-User Devices #7: Email and Web Browser Protections #11: Secure Configurations for Network Devices	
MA-5	**Maintenance Personnel**	A.9.4.5, A.11.2.4	040204, 040405, 041107, 050103		§§164.308(a)(3)(ii)(A) 164.310(a)(2)(iv)	BAI09.03		
MA-6	**Timely Maintenance**	A.11.2.4	040201, 040204, 040205, 040206, 040501, 040509, 041107					
Media Protection (MP)								
MP-1	**Media Protection Policy and Procedures**	A.5.1.1, A.5.1.2, A.6.1.1, A.9.1.1, A.12.1.1, A.18.1.1, A.18.1.3, A.18.2.2	010101	MP-1 (b) (1) MP-1 (b) (2)				

NIST Control ID	NIST Control Name	ISO 27001/2:2013	2016 SISM	FedRAMP	HIPAA Security Rule 45 C.F.R.	COBIT 5	CIS Critical Security Controls v6.1: 2016	FERPA Privacy Technical Assistance Center (PTAC) Data Security Checklist
MP-2	**Media Access**	A.7.1.2, A.8.2.2, A.8.2.3, A.8.3.1, A.11.2.9	020101, 020102, 030102, 030201, 030501, 030502, 030503		§§164.308(a)(3)(i), 164.308(a)(3)(ii)(A), 164.310(d)(1), 164.310(d)(2), 164.312(a)(1), 164.312(a)(2)(iv), 164.312(b)	SS05.02, APO13.01	#6: Maintenance, Monitoring, and Analysis of Audit Logs #13: Data Protection	
MP-3	**Media Marking**	A.7.1.2, A.8.2.2, A.8.2.3, A.8.3.1	010101, 041301, 041302				#14: Controlled Access Based on the Need to Know	
MP-4	**Media Storage**	A.8.2.3, A.8.3.1, A.11.2.9, A.18.1.3	040509, 041201, 041301		§§164.308(a)(3)(i), 164.308(a)(3)(ii)(A), 164.310(d)(1), 164.310(d)(2), 164.312(a)(1), 164.312(a)(2)(iv), 164.312(b)	DSS05.02, APO13.01	#6: Maintenance, Monitoring, and Analysis of Audit Logs #10: Data Recovery Capability	
MP-5	**Media Transport**	A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.5, A.11.2.6	041301		§§164.308(a)(3)(i), 164.308(a)(3)(ii)(A), 164.310(d)(1), 164.310(d)(2), 164.312(a)(1), 164.312(a)(2)(iv), 164.312(b)	DSS05.02, APO13.01	#6: Maintenance, Monitoring, and Analysis of Audit Logs #13: Data Protection	
MP-6	**Media Sanitization**	A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7	040208, 041103		§§164.308(a)(1)(ii)(A) 164.310(a)(2)(ii), 164.310(a)(2)(iii), 164.310(a)(2)(iv), 164.310(d)(1), 164.310(d)(2), 164.310(d)(2)(i), 164.310(d)(2)(ii)	BAI09.03	#6: Maintenance, Monitoring, and Analysis of Audit Logs	
MP-7	**Media Use**	A.8.2.3, A.8.3.1	020101, 020201, 030102, 030302, 041001		§§164.308(a)(3)(i), 164.308(a)(3)(ii)(A), 164.310(d)(1), 164.310(d)(2), 164.312(a)(1), 164.312(a)(2)(iv), 164.312(b)	APO13.01, DSS05.02	#6: Maintenance, Monitoring, and Analysis of Audit Logs	
MP-8	**Media Downgrading**	A.8.2.3, A.8.3.1						
Physical & Environmental Protection PE)								
PE-1	**Physical and Environmental Protection Policy and Procedures**	A.5.1.1, A.5.1.2, A.6.1.1, A.9.2.1, A.11.1.4, A.11.2.1, A.11.2.2, A.12.1.1, A.18.1.1, A.18.2.2		PE-1 (b) (1) PE-1 (b) (2)				
PE-2	**Physical Access Authorizations**	A.9.2.1, A.9.2.5, A.11.1.2, A.11.1.5	050103, 060102	PE-2	§§164.308(a)(1)(ii)(B), 164.308(a)(7)(i), 164.308(a)(7)(ii)(A), 164.310(a)(1), 164.310(a)(2)(i), 164.310(a)(2)(ii), 164.310(a)(2)(iii), 164.310(b), 164.310(c), 164.310(d)(1), 164.310(d)(2)(iii)	DSS01.04, DSS05.05		

NIST Control ID	NIST Control Name	ISO 27001/2:2013	2016 SISM	FedRAMP	HIPAA Security Rule 45 C.F.R.	COBIT 5	CIS Critical Security Controls v6.1: 2016	FERPA Privacy Technical Assistance Center (PTAC) Data Security Checklist
PE-3	**Physical Access Control**	A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.5, A.11.1.6, A.11.2.8	020101, 030402, 040501, 040906, 041001, 041002, 041005, 050101, 050103, 050104, 050105, 050201, 050202, 050203	PE-3 (a) (2) PE-3 (d) PE-3 (f) PE-3 (g)	§§164.306(e), 164.308(a)(1)(ii)(B), 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(7)(i), 164.308(a)(7)(ii)(A), 164.310(a)(1), 164.310(a)(2)(i), 164.310(a)(2)(ii), 164.310(a)(2)(iii), 164.310(b), 164.310(c), 164.310(d)(1), 164.310(d)(2)(iii), 164.312(b), 164.314(b)(2)(i)	APO13.02, DSS01.04, DSS05.05		Make computing resources physically unavailable to unauthorized users. This includes securing access to any areas where sensitive data are stored and processed.
PE-4	**Access Control for Transmission Medium**	A.11.1.2, A.11.1.3, A.11.1.5, A.11.2.3	040905, 050103		§§164.308(a)(1)(ii)(B), 164.308(a)(7)(i), 164.308(a)(7)(ii)(A), 164.310(a)(1), 164.310(a)(2)(i), 164.310(a)(2)(ii), 164.310(a)(2)(iii), 164.310(b), 164.310(c), 164.310(d)(1),	DSS01.04, DSS05.05		
PE-5	**Access Control for Output Devices**	A.11.1.2, A.11.1.3, A.11.2.8, A.13.1.1	020103, 040906		§§164.308(a)(1)(ii)(B), 164.308(a)(7)(i), 164.308(a)(7)(ii)(A), 164.310(a)(1), 164.310(a)(2)(i), 164.310(a)(2)(ii), 164.310(a)(2)(iii), 164.310(b), 164.310(c), 164.310(d)(1),			
PE-6	**Monitoring Physical Access**	A.11.1.2, A.11.1.5, A.12.1.2	050101, 050105	PE-6 (b)	§§164.308(a)(1)(i), 164.308(a)(1)(ii)(B), 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(6)(ii), 164.308(a)(7)(i), 164.308(a)(7)(ii)(A), 164.310(a)(1), 164.310(a)(2)(i), 164.310(a)(2)(ii), 164.310(a)(2)(iii), 164.310(b), 164.310(c), 164.310(d)(1), 164.310(d)(2)(iii), 164.312(b), 164.314(a)(2)(i)(C), 164.314(b)(2)(i)	DSS01.04, DSS02.07, DSS05.05		Monitor access to these areas to prevent intrusion attempts (e.g., by administering identification badges and requiring staff and visitors to log in prior to entering the premises or accessing the resources).
PE-7	**Visitor Control**	**Withdrawn: Incorporated into PE-2 and PE-3**						
PE-8	**Visitor Access Records**	A.11.1.5, A.12.1.2, A.18.2.2	050103	PE-8 (a) PE-8 (b)				

NIST Control ID	NIST Control Name	ISO 27001/2:2013	2016 SISM	FedRAMP	HIPAA Security Rule 45 C.F.R.	COBIT 5	CIS Critical Security Controls v6.1: 2016	FERPA Privacy Technical Assistance Center (PTAC) Data Security Checklist
PE-9	**Power Equipment and Cabling**	A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3	040901, 040902, 040905		§§164.308(a)(1)(ii)(B), 164.308(a)(7)(i), 164.308(a)(7)(ii)(A), 164.308.(a)(7)(ii)(E), 164.310(a)(1), 164.310(a)(2)(i), 164.310(a)(2)(iii), 164.310(b), 164.310(c), 164.310(d)(1), 164.310(d)(2)(iii), 164.312(a)(2)(ii), 164.314(a)(1),	DSS01.04, DSS05.05		
PE-10	**Emergency Shutoff**	A.11.1.4, A.11.2.2			§§164.308(a)(7)(i), 164.308(a)(7)(ii)(C), 164.310, 164.316(b)(2)(iii)	DSS01.04, DSS05.05		
PE-11	**Emergency Power**	A.11.1.4, A.11.2.2	030101, 040901, 040902		§§164.308(a)(7)(i), 164.308.(a)(7)(ii)(E), 164.310(a)(2)(i), 164.312(a)(2)(ii), 164.314(a)(1), 164.314(b)(2)(i)			
PE-12	**Emergency Lighting**	A.11.2.2	040901		§§164.308(a)(7)(i), 164.308(a)(7)(ii)(C), 164.310, 164.316(b)(2)(iii)	DSS01.04, DSS05.05		
PE-13	**Fire Protection**	A.11.1.4, A.11.2.1	050101, 050102, 050106, 050202, 050203		§§164.308(a)(7)(i), 164.308(a)(7)(ii)(C), 164.310, 164.316(b)(2)(iii)	DSS01.04, DSS05.05		
PE-14	**Temperature and Humidity Controls**	A.11.1.4, A.11.2.1, A.11.2.2	050102, 050202	PE-14 (a) PE-14 (b)	§§164.308(a)(7)(i), 164.308(a)(7)(ii)(C), 164.310, 164.316(b)(2)(iii)	DSS01.04, DSS05.05		
PE-15	**Water Damage Protection**	A.11.1.4, A.11.2.1, A.11.2.2	050101, 050102, 050106, 050202, 050203		§§164.308(a)(7)(i), 164.308(a)(7)(ii)(C), 164.310, 164.316(b)(2)(iii)	DSS01.04, DSS05.05		
PE-16	**Delivery and Removal**	A.8.2.3, A.8.3.1, A.11.1.6, A.11.2.5	041106, 050101	PE-16	§§164.308(a)(1)(ii)(A), 164.310(a)(2)(ii), 164.310(a)(2)(iii), 164.310(a)(2)(iv), 164.310(d)(1), 164.310(d)(2)	BAI09.03		
PE-17	**Alternate Work Site**	A.6.2.2, A.11.2.6, A.13.2.1	041003					
PE-18	**Location of Information System Components**	A.8.2.3, A.11.1.4, A.11.2.1, A.11.2.8	050101		§§164.308(a)(7)(i), 164.308(a)(7)(ii)(C), 164.310, 164.316(b)(2)(iii)	DSS01.04, DSS05.05		
PE-19	**Information Leakage**	A.11.1.4, A.11.2.1	040905		§§164.308(a)(1)(ii)(D), 164.308(a)(3), 164.308(a)(4), 164.310(b), 164.310(c), 164.312(a),			

NIST Control ID	NIST Control Name	ISO 27001/2:2013	2016 SISM	FedRAMP	HIPAA Security Rule 45 C.F.R.	COBIT 5	CIS Critical Security Controls v6.1: 2016	FERPA Privacy Technical Assistance Center (PTAC) Data Security Checklist
PE-20	**Asset Monitoring and Tracking**	A.8.2.3	041101		§§164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.310(a)(1), 164.310(a)(2)(ii), 164.310(a)(2)(iii), 164.310(b), 164.310(c), 164.310(d)(1), 164.310(d)(2)(iii), 164.312(b), 164.314(b)(2)(i)			
Planning (PL)								
PL-1	**Security Planning Policy and Procedures**	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2		PL-1 (b) (1) PL-1 (b) (2)				Policy and governance - organizational policies and standards regarding data security and individual privacy protection
PL-2	**System Security Plan**	A.14.1.1		PL-2 (c)	§§164.306(e), 164.308(a)(7)(ii)(D), 164.308(a)(8), 164.316(b)(2)(iii)	APO11.06, DSS04.05		
PL-3	**System Security Plan Update**	**Withdrawn: Incorporated into PL-2**						
PL-4	**Rules of Behavior**	A.6.1.1, A.6.2.1, A.6.2.2, A.7.1.2, A.7.2.1, A.8.1.3, A.11.1.5, A.13.2.1, A.13.2.4, A.16.1.3	010201, 020201, 030302	PL-4 (c)			#19: Incident Response and Management	Personnel security - policies and guidelines concerning personal and work-related use of Internet, Intranet, and extranet systems
PL-5	**Privacy Impact Assessment**	**Withdrawn: Incorporated into Appendix J, AR-2, RA-3**						
PL-6	**Security Related Activity Planning**	**Withdrawn: Incorporated into PL-2**						
PL-7	**Security Concept of Operations**	A.14.1.1						
PL-8	**Information Security Architecture**	A.14.1.1			§§164.308(a)(1)(i), 164.308(a)(1)(ii)(A), 164.308(a)(3)(ii)(A), 164.308(a)(8), 164.310(d)	APO13.01		
PL-9	**Central Management**							
Program Management (PM)								
PM-1	**Information Security Program Plan**	A.5.1.1, A.5.1.2, A.6.1.1, A.18.1.1, A.18.2.2			§§164.308(a)(1)(i), 164.308(a)(2), 164.308(a)(3), 164.308(a)(4), 164.314, 164.316	APO13.12		
PM-2	**Senior Information Security Officer**	A.6.1.1						
PM-3	**Information Security Resources**							
PM-4	**Plan of Action and Milestones Process**	A.12.5.1			§§164.308(a)(1)(ii)(B), 164.314(a)(2)(i)(C), 164.314(b)(2)(iv)	APO12.05, APO13.02		
PM-5	**Information System Inventory**	A.8.1.1, A.8.1.2						
PM-6	**Information Security Measures of Performance**				§§164.306(e), 164.308(a)(7)(ii)(D), 164.308(a)(8), 164.316(b)(2)(iii)	APO11.06, DSS04.05		
PM-7	**Enterprise Architecture**							

NIST Control ID	NIST Control Name	ISO 27001/2:2013	2016 SISM	FedRAMP	HIPAA Security Rule 45 C.F.R.	COBIT 5	CIS Critical Security Controls v6.1: 2016	FERPA Privacy Technical Assistance Center (PTAC) Data Security Checklist
PM-8	**Critical Infrastructure Plan**				§§164.308(a)(1)(ii)(A) 164.308(a)(1)(ii)(B), 164.308(a)(4)(ii), 164.308(a)(6)(ii), 164.308(a)(7)(i), 164.308(a)(7)(ii)(C), 164.308(a)(7)(ii)(E), 164.308(a)(8), 164.310(a)(2)(i), 164.314, 164.316	APO02.06, APO03.01		Layered defense - Protect hosts (individual computers), application, network, and perimeter.
PM-9	**Risk Management Strategy**				§§164.308(a)(1), 164.308(a)(1)(i), 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.314(a)(2)(i)(C), 164.308(a)(6), 164.308(a)(7)(ii)(E), 164.308(a)(8), 164.308(b), 164.314(b)(2)(iv), 164.316(a)	APO12.02, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03, BAI04.02, DSS04.02		
PM-10	**Security Authorization Process**	A.6.1.1						
PM-11	**Mission/Business Process Definition**				§§164.308(a)(1), 164.308(a)(1)(i), 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(2), 164.308(a)(3), 164.308(a)(4), 164.308(a)(6), 164.308(a)(7)(ii)(B), 164.308(a)(7)(ii)(C), 164.308(a)(7)(ii)(D), 164.308(a)(7)(ii)(E), 164.308(a)(8), 164.308(b), 164.308(b)(1), 164.310(a)(2)(i), 164.314, 164.316, 164.316(a)	APO01.02, APO02.01, APO02.06, APO03.01, DSS04.02, DSS06.03		
PM-12	**Insider Threat Program**				§§164.308(a)(1)(ii)(A) 164.308(a)(1)(ii)(D), 164.308(a)(3), 164.308(a)(4), 164.308(a)(5)(ii)(A), 164.310(a)(1), 164.310(a)(2)(iii), 164.312(a)(1), 164.312(c), 164.312(e), 164.314, 164.316	APO12.01, APO12.02, APO12.03, APO12.04		

NIST Control ID	NIST Control Name	ISO 27001/2:2013	2016 SISM	FedRAMP	HIPAA Security Rule 45 C.F.R.	COBIT 5	CIS Critical Security Controls v6.1: 2016	FERPA Privacy Technical Assistance Center (PTAC) Data Security Checklist
PM-13	**Information Security Workforce**	A.7.2.1, A.7.2.2			§§164.308(a)(2), 164.308(a)(3)(i), 164.308(a)(5), 164.308(a)(5)(i), 164.308(a)(5)(ii)(A), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(5)(ii)(D), 164.530(b)(1)	APO07.02, APO07.03, BAI05.07, DSS06.03	#17: Security Skills Assessment and Appropriate Training	
PM-14	**Testing, Training, and Monitoring**	A.7.2.1			§§164.306(e), 164.308(a)(1)(i), 164.308(a)(2), 164.308(a)(3)(ii)(A), 164.308(a)(3)(ii)(B), 164.308(a)(4), 164.308(a)(7)(ii)(D), 164.308(a)(8), 164.310(a)(2)(iii), 164.312(a)(1), 164.312(a)(2)(ii)	APO11.06, DSS04.05, DSS05.01		
PM-15	**Contacts with Security Groups and Associations**	A.6.1.4			§§164.308(a)(6), 164.308(a)(7)(i), 164.308(a)(7)(ii)(C), 164.310, 164.316(b)(2)(iii)			
PM-16	**Threat Awareness Program**				§§164.308(a)(1)(ii)(A) 164.308(a)(1)(ii)(B), 164.308(a)(1)(ii)(D), 164.308(a)(3), 164.308(a)(4), 164.308(a)(5)(ii)(A), 164.308(a)(7)(ii)(D), 164.308(a)(7)(ii)(E), 164.310(a)(1), 164.310(a)(2)(iii), 164.312(a)(1), 64.312(c), 164.312(e), 164.314, 164.316, 164.316(a)	APO12.01, APO12.02, APO12.03, APO12.04		
Personnel Security (PS)								
PS-1	**Personnel Security Policy and Procedures**			PS-1 (b) (1) PS-1 (b) (2)	§§164.308(a)(1)(ii)(C), 164.308(a)(3)			
PS-2	**Position Risk Designation**	A.6.1.1		PS-2 (c)	§§164.308(a)(1)(ii)(C), 164.308(a)(3)			
PS-3	**Personnel Screening**	A.7.1.1		PS-3 (b)	§§164.308(a)(1)(ii)(C), 164.308(a)(1)(ii)(D), 164.308(a)(3), 164.308(a)(4), 164.310(b), 164.310(c), 164.312(a),	APO01.06		Confirm the trustworthiness of employees through the use of personnel security screenings, policy training, and binding confidentiality agreements.
PS-4	**Personnel Termination**	A.7.3.1, A.9.2.6		PS-4 (a)	§§164.308(a)(1)(ii)(C), 164.308(a)(3)			
PS-5	**Personnel Transfer**	A.7.3.1, A.9.2.6		PS-5 (d)-2	§§164.308(a)(1)(ii)(C), 164.308(a)(3)			

NIST Control ID	NIST Control Name	ISO 27001/2:2013	2016 SISM	FedRAMP	HIPAA Security Rule 45 C.F.R.	COBIT 5	CIS Critical Security Controls v6.1: 2016	FERPA Privacy Technical Assistance Center (PTAC) Data Security Checklist
PS-6	**Access Agreements**	A.6.1.1, A.6.2.1, A.6.2.2, A.7.2.1, A.11.1.5, A.13.2.1, A.13.2.4	020201	PS-6 (b) PS-6 (c) (2)	§§164.308(a)(1)(ii)(C), 164.308(a)(1)(ii)(D), 164.308(a)(3), 164.308(a)(4), 164.310(b), 164.310(c), 164.312(a),	APO01.06		Conduct regular checks and trainings to ensure employee understanding of the terms and conditions of their employment
PS-7	**Third-Party Personnel Security**	A.6.1.1, A.7.2.1, A.15.1.1, A.15.1.2		PS-7 (d)-2	§§164.308(a)(1)(i), 164.308(a)(1)(ii)(C), 164.308(a)(1)(ii)(D), 164.308(a)(2), 164.308(a)(3), 164.308(a)(4), 164.308(b), 164.308(b)(1), 164.314, 164.314(a)(1), 164.314(a)(2)(i), 164.314(a)(2)(ii), 164.316	APO01.02, APO07.03, APO07.06, APO10.04, APO10.05, APO13.12, DSS06.03	#17: Security Skills Assessment and Appropriate Training	
PS-8	**Personnel Sanctions**	A.7.2.3			§§164.308(a)(1)(ii)(C), 164.308(a)(3)			
				Risk Assessment (RA)				
RA-1	**Risk Assessment Policy and Procedures**	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2	070201	RA-1 (b) (1) RA-1 (b) (2)				
RA-2	**Security Categorization**	A.8.2.1	070201		§§164.308(a)(1)(i), 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(1)(ii)(D), 164.308(a)(6), 164.308(a)(7)(ii)(D), 164.308(a)(7)(ii)(E), 164.308(a)(8), 164.316(a)	APO03.03, APO03.04, APO12.02, BAI09.02, DSS04.02	#14: Controlled Access Based on the Need to Know	
RA-3	**Risk Assessment**	A.12.6.1, A.15.2.2	070202, 070203	RA-3 (b) RA-3 (c) RA-3 (d) RA-3 (e)	§§164.308(a)(1)(i), 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(1)(ii)(D), 164.308(a)(3), 164.308(a)(4), 164.308(a)(5)(ii)(A), 164.308(a)(6), 164.308(a)(6)(ii), 164.308(a)(7)(ii)(E), 164.308(a)(8), 164.310(a)(1), 164.310(a)(2)(iii), 164.312(a)(1), 164.312(c), 164.312(e), 164.314, 164.316, 164.316(a), 164.316(b)(2)(iii)	APO12.01, APO12.02, APO12.03, APO12.04, APO12.06, DSS04.02	#4: Continuous Vulnerability Assessment and Remediation	
RA-4	**Risk Assessment Update**	**Withdrawn: Incorporated into RA-3**						

NIST Control ID	NIST Control Name	ISO 27001/2:2013	2016 SISM	FedRAMP	HIPAA Security Rule 45 C.F.R.	COBIT 5	CIS Critical Security Controls v6.1: 2016	FERPA Privacy Technical Assistance Center (PTAC) Data Security Checklist
RA-5	**Vulnerability Scanning**	A.12.6.1, A.18.2.3	040201, 040906, 060102	RA-5 (a) RA-5 (d) RA-5 (e)	§§164.306(e), 164.308(a)(1)(i), 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(6)(ii), 164.308(a)(7)(ii)(E), 164.308(a)(8), 164.310(a)(1), 164.312(a)(1), 164.314(a)(2)(i)(C), 164.314(a)(2)(iii), 164.316(b)(2)(iii)	APO12.01, APO12.02, APO12.03, APO12.04, BAI03.10	#3: Secure Configuration for End-User Devices #4: Continuous Vulnerability Assessment and Remediation #7: Email and Web Browser Protections	Continuous scanning - Ensure network components remain in a secure state to enhance data security protection. Automated vulnerability scanning - Scan network for new new vulnerabilities (to hardware, operating systems, applications, and other network devices) on a regular basis will minimize the time of exposure to known vulnerabilities.
RA-6	**Technical Surveillance Countermeasures Survey**						#20: Penetration Tests and Red Team Exercises	
System & Services Acquisition (SA)								
SA-1	**System and Services Acquisition Policy and Procedures**	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.14.1.1, A.14.2.7, A.18.1.1, A.18.2.2		SA-1 (b) (1) SA-1 (b) (2)				
SA-2	**Allocation of Resources**		040403, 040501					
SA-3	**System Development Life Cycle**	A.6.1.1, A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.6	040101, 040303, 040304, 040401		§§164.308(a)(1)(i)	APO13.01	#6: Maintenance, Monitoring, and Analysis of Audit Logs	
SA-4	**Acquisition Process**	A.14.1.1, A.14.2.7, A.14.2.9, A.15.1.2	010202, 040101, 040401, 040603, 040701, 040801, 040802	SA-4	§§164.308(a)(1)(i), 164.308(a)(1)(ii)(D)	APO07.06, APO13.01	#1: Inventory of Authorized and Unauthorized Devices #2: Inventory of Authorized and Unauthorized Software #3: Secure Configuration for End-User Devices #6: Maintenance, Monitoring, and Analysis of Audit Logs #7: Email and Web Browser Protections	
SA-5	**Information System Documentation**	A.12.1.1, A.18.1.3	040102, 040202, 040203, 040205, 040405, 040407, 040509, 041101		§§164.308(a)(1)(ii)(A) 164.308(a)(7)(ii)(E), 164.308(a)(8), 164.310(a)(1), 164.312(a)(1), 164.316(b)(2)(iii)	APO12.01, APO12.02, APO12.03, APO12.04		
SA-6	**Software Usage Restrictions**	**Withdrawn: Incorporated into CM-10 and SI-7**						
SA-7	**User Installed Software**	**Withdrawn: Incorporated into CM-11 and SI-7**						
SA-8	**Security Engineering Principles**	A.12.2.1, A.13.1.3, A.14.2.5, A.14.2.7	040303, 040401		§§164.308(a)(1)(i)	APO13.01	#19: Secure Network Engineering	
SA-9	**External Information System Services**	A.6.1.1, A.6.1.5, A.7.2.1, A.11.2.5, A.11.2.6, A.13.1.2, A.13.2.2, A.13.2.4, A.14.2.7, A.15.1.1, A.15.1.2, A.15.2.1, A.15.2.2	030602, 041401, 041402, 041403	SA-9 (a) SA-9 (c)	§§164.308(a)(1)(ii)(D), 164.308(a)(4)(ii)(A), 164.308(b), 164.314(a)(1), 164.314(a)(2)(i), 164.314(a)(2)(i)(B), 164.314(a)(2)(ii), 164.316(b)(2)	APO02.02, APO07.03, APO10.04, APO10.05	#9: Limitation and Control of Network Ports, Protocols and Service #12: Boundary Defense #19: Incident Response and Management	
SA-10	**Developer Configuration Management**	A.9.4.5, A.12.1.2, A.14.2.2, A.14.2.4, A.14.2.7, A.15.2.2	040301, 040302, 040303, 040304		§§164.308(a)(1)(i), 164.308(a)(8), 164.308(a)(7)(i), 164.308(a)(7)(ii)	BAI01.06, BAI06.01, BAI10.01, BAI10.02, BAI10.03, BAI10.05	#3: Secure Configuration for End-User Devices #6: Maintenance, Monitoring, and Analysis of Audit Logs	

NIST Control ID	NIST Control Name	ISO 27001/2:2013	2016 SISM	FedRAMP	HIPAA Security Rule 45 C.F.R.	COBIT 5	CIS Critical Security Controls v6.1: 2016	FERPA Privacy Technical Assistance Center (PTAC) Data Security Checklist
SA-11	**Developer Security Testing and Evaluation**	A.14.2.7, A.14.2.8, A.14.2.9	040207, 040601, 040602		§§164.308(a)(1)(i), 164.308(a)(1)(ii)(A), 164.308(a)(7)(ii)(E), 164.308(a)(8), 164.310(a)(1), 164.312(a)(1), 164.316(b)(2)(iii)	APO12.01, APO12.02, APO12.03, APO12.04, APO13.01	#3: Secure Configuration for End-User Devices #4: Continuous Vulnerability Assessment and Remediation #6: Maintenance, Monitoring, and Analysis of Audit Logs #17: Security Skills Assessment and Appropriate Training #20: Penetration Tests and Red Team Exercises	
SA-12	**Supply Chain Protections**	A.14.2.7, A.15.1.1, A.15.1.2, A.15.1.3	030202, 030305, 030308, 040102, 040202, 060105		§§164.308(a)(1)(i), 164.308(a)(1)(ii)(A), 164.308(a)(4)(ii), 164.308(a)(7)(ii)(C), 164.308(a)(7)(ii)(E), 164.308(a)(8), 164.310(a)(2)(i), 164.314, 164.316	APO08.04, APO08.05, APO10.03, APO10.04, APO10.05, APO13.01	#6: Maintenance, Monitoring, and Analysis of Audit Logs	
SA-13	**Trustworthiness**	A.14.2.7					#18: Application Software Security	
SA-14	**Criticality Analysis**				§§164.308(a)(1)(i), 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(6), 164.308(a)(6)(ii), 164.308(a)(7), 164.308(a)(7)(ii)(B), 164.308(a)(7)(ii)(C), 164.308(a)(7)(ii)(D), 164.308(a)(7)(ii)(E), 164.308(a)(8), 164.310(a)(2)(i), 164.312(a)(2)(ii), 164.314(b)(2)(i), 164.316, 164.316(a)	APO02.01, APO02.06, APO03.01, APO03.03, APO03.04, BAI09.02, DSS04.02		
SA-15	**Development Process, Standards, and Tools**	A.6.1.5, A.14.2.1, A.14.2.7, A.14.2.9			§§164.308(a)(1)(i)	APO13.01	#6: Maintenance, Monitoring, and Analysis of Audit Logs #18: Application Software Security	
SA-16	**Developer-Provided Training**						#17: Security Skills Assessment and Appropriate Training #18: Application Software Security	
SA-17	**Developer Security Architecture and Design**	A.14.2.1, A.14.2.5, A.14.2.7			§§164.308(a)(1)(i)	APO13.01	#6: Maintenance, Monitoring, and Analysis of Audit Logs #18: Application Software Security #19: Secure Network Engineering	
SA-18	**Tamper Resistance and Detection**		030308				#13: Data Protection	
SA-19	**Component Authenticity**							
SA-20	**Customized Development of Critical Components**						#18: Application Software Security	
SA-21	**Developer Screening**	A.7.1.1					#18: Application Software Security	
SA-22	**Unsupported System Components**		040101, 040204					
System & Communications Protection (SC)								
SC-1	**System and Communications Protection Policy and Procedures**	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2		SC-1 (b) (1) SC-1 (b) (2)				
SC-2	**Application Partitioning**	A.12.2.1	030101, 030104					
SC-3	**Security Function Isolation**	A.12.2.1, A.14.1.2						

NIST Control ID	NIST Control Name	ISO 27001/2:2013	2016 SISM	FedRAMP	HIPAA Security Rule 45 C.F.R.	COBIT 5	CIS Critical Security Controls v6.1: 2016	FERPA Privacy Technical Assistance Center (PTAC) Data Security Checklist
SC-4	**Information In Shared Resources**							
SC-5	**Denial of Service Protection**		060103, 060104		§§164.308(a)(1)(ii)(A) 164.308(a)(1)(ii)(B), 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(7), 164.308(a)(8), 164.310(a)(2)(i), 164.310(d)(2)(iv), 164.312(a)(2)(ii), 164.312(b), 164.312(e)(2)(i)	APO13.01, DSS05.07		
SC-6	**Resource Availability**		040103, 040509, 040901, 041202, 060103					
SC-7	**Boundary Protection**	A.12.1.2, A.12.2.1, A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3	030101, 030105		§§164.308(a)(1)(ii)(D), 164.308(a)(3), 164.308(a)(4), 164.308(a)(4)(ii)(B), 164.310(a)(1), 164.310(b), 164.310(c), 164.312(a), 164.312(a)(1), 164.312(b), 164.312(c), 164.312(e)	APO01.06, APO13.01, DSS05.02, DSS05.07	#1: Inventory of Authorized and Unauthorized Devices #5: Controlled Use of Administrative Privileges #11: Secure Configurations for Network Devices #9: Limitation and Control of Network Ports, Protocols and Service #12: Boundary Defense #19: Secure Network Engineering	Firewalls and Intrusion Detection/Prevention Systems (IDPS) - Protect networks from unauthorized access, while permitting legitimate communications to pass. Use an IDPS to detect malicious activity on the network.
SC-8	**Transmission Confidentiality and Integrity**	A.8.2.3, A.10.1.1, A.13.1.1, A.13.1.2, A.13.2.1, A.13.2.2, A.13.2.3, A.14.1.2, A.14.1.3	030201, 030301, 040505, 040904, 040905		§§164.308(a)(1)(ii)(D), 164.308(a)(3), 164.308(a)(4), 164.308(b)(1), 164.308(b)(2), 164.310(b), 164.310(c), 164.312(a), 164.312(e) 164.312(e)(1), 164.312(e)(2)(i), 164.312(e)(2)(ii),	APO01.06, DSS06.06	#1: Inventory of Authorized and Unauthorized Devices #5: Controlled Use of Administrative Privileges #8: Malware Defenses #11: Secure Configurations for Network Devices #9: Limitation and Control of Network Ports, Protocols and Service #12: Boundary Defense #13: Data Protection #15: Wireless Access Control	
SC-9	**Transmission Confidentiality**	**Withdrawn: Incorporated into SC-8**						
SC-10	**Network Disconnect**	A.9.4.2, A.11.2.8, A.13.1.1	020108, 030107				#1: Inventory of Authorized and Unauthorized Devices #11: Secure Configurations for Network Devices #12: Boundary Defense	
SC-11	**Trusted Path**		030101					
SC-12	**Cryptographic Key Establishment and Management**	A.10.1.1, A.10.1.2	030501, 030502, 040505, 040507, 041201	SC-12			#13: Data Protection	
SC-13	**Cryptographic Protection**	A.10.1.1, A.14.1.2, A.14.1.3, A.18.1.5	020101, 020108, 030201, 030501	SC-13	§§164.308(a)(1)(ii)(D), 164.308(a)(3), 164.308(a)(4), 164.310(b), 164.310(c), 164.312(a),	APO01.06	#15: Wireless Access Control #10: Data Recovery Capability #6: Maintenance, Monitoring, and Analysis of Audit Logs #13: Data Protection	
SC-14	**Public Access Protections**	**Withdrawn: Capability provided by AC-2, AC-3, AC-5, AC-6, SI-3, SI-4, SI-5, SI-7, SI-10**						
SC-15	**Collaborative Computing Devices**	A.13.2.1		SC-15 (a)			#3: Secure Configuration for End-User Devices #7: Email and Web Browser Protections	

NIST Control ID	NIST Control Name	ISO 27001/2:2013	2016 SISM	FedRAMP	HIPAA Security Rule 45 C.F.R.	COBIT 5	CIS Critical Security Controls v6.1: 2016	FERPA Privacy Technical Assistance Center (PTAC) Data Security Checklist
SC-16	**Transmission of Security Attributes**	A.7.1.2, A.8.2.2, A.13.2.1	030106				#14: Controlled Access Based on the Need to Know	
SC-17	**Public Key Infrastructure Certificates**	A.10.1.2					#1: Inventory of Authorized and Unauthorized Devices #13: Data Protection #15: Wireless Access Control #16: Account Monitoring and Control	
SC-18	**Mobile Code**		030308		§§164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B)		#2: Inventory of Authorized and Unauthorized Software	
SC-19	**Voice Over Internet Protocol**	A.13.1.1	030401					
SC-20	**Secure Name/Address Resolution Service (Authoritative Source)**	A.13.1.1	030101				#9: Limitation and Control of Network Ports	
SC-21	**Secure Name/Address Resolution Service (Recursive or Caching Resolver)**	A.13.1.1	030101				#9: Limitation and Control of Network Ports	
SC-22	**Architecture and Provisioning for Name/Address Resolution Service**	A.13.1.1	030101				#9: Limitation and Control of Network Ports	
SC-23	**Session Authenticity**	A.13.1.1	020108, 030102, 030105				#16: Account Monitoring and Control	
SC-24	**Fail in Known State**		040505, 040506, 040507				#11: Secure Configurations for Network Devices	
SC-25	**Thin Nodes**							
SC-26	**Honeypots**							
SC-27	**Platform-Independent Applications**							
SC-28	**Protection of Information at Rest**	A.8.2.3	030104, 030501, 030601		§§164.308(a)(1)(ii)(D), 164.308(b)(1), 164.310(d), 164.312(a)(1), 164.312(a)(2)(iii), 164.312(a)(2)(iv), 164.312(b), 164.312(c), 164.314(b)(2)(i), 164.312(d)	APO01.06, BAI02.01, BAI06.01, DSS06.06	#13: Data Protection	
SC-29	**Heterogeneity**		030103, 060102					
SC-30	**Concealment and Misdirection**							
SC-31	**Covert Channel Analysis**				§§164.308(a)(1)(ii)(D), 164.308(a)(3), 164.308(a)(4), 164.310(b), 164.310(c), 164.312(a),	APO01.06	#13: Data Protection	
SC-32	**Information System Partitioning**		030104, 040906					
SC-33	**Transmission Preparation Integrity**	**Withdrawn: Incorporated into SC-8**						
SC-34	**Non-Modifiable Executable Programs**						#2: Inventory of Authorized and Unauthorized Software #3: Secure Configuration for End-User Devices #4: Continuous Vulnerability Assessment and Remediation #7: Email and Web Browser Protections	
SC-35	**Honeyclients**							

NIST Control ID	NIST Control Name	ISO 27001/2:2013	2016 SISM	FedRAMP	HIPAA Security Rule 45 C.F.R.	COBIT 5	CIS Critical Security Controls v6.1: 2016	FERPA Privacy Technical Assistance Center (PTAC) Data Security Checklist
SC-36	**Distributed Processing and Storage**							
SC-37	**Out-of-Band Channels**		020108					
SC38	**Operations Security**	A.12.x	040501, 040509					
SC-39	**Process Isolation**						#8: Malware Defenses #18: Application Software Security	
SC-40	**Wireless Link Protection**		030501, 030701				#15: Wireless Access Control	
SC-41	**Port and I/O Device Access**		020201				#9: Limitation and Control of Network Ports #13: Data Protection	
SC-42	**Sensor Capability and Data**	A.12.2.1						
SC-43	**Usage Restrictions**		020201					
SC-44	**Detonation Chambers**				§§164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B)		#8: Malware Defenses	
System & Information Integrity (SI)								
SI-1	**System and Information Integrity Policy and Procedures**	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2		SI-1 (b) (1) SI-1 (b) (2)				
SI-2	**Flaw Remediation**	A.12.6.1, A.14.2.2, A.14.2.3, A.16.1.3	030101, 040201, 040401, 040402, 040509	SI-2 (c)	§§164.308(a)(1)(i), 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(7)(ii)(E), 164.308(a)(8), 164.310(a)(1), 164.312(a)(1), 164.316(b)(2)(iii)	APO12.01, APO12.02, APO12.03, APO12.04	#3: Secure Configuration for End-User Devices #4: Continuous Vulnerability Assessment and Remediation #7: Email and Web Browser Protections	Patch management - Use a strategy and plan for what patches should be applied to which systems at a specified time. Used in conjunction with vulnerability scanning to quickly shut down any vulnerability discovered.
SI-3	**Malicious Code Protection**	A.12.2.1	020108, 030103, 030301, 030303, 030306, 041003, 060104, 060105	SI-3 (c) (1)-1 SI-3 (c) (1)-2 SI-3 (c) (2)	§§164.306(e), 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B)	APO13.02, DSS05.01	#8: Malware Defenses	
SI-4	**Information System Monitoring**	A.12.1.2, A.16.1.2, A.16.1.3	030503, 040510, 060102	SI-4	§§164.306(e), 164.308(a)(1)(i), 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(D), 164.308(a)(3), 164.308(a)(4), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(6)(i), 164.308(a)(6)(ii), 164.308(a)(7)(ii)(E), 164.308(a)(8), 164.310(a)(1), 164.310(a)(2)(ii), 164.310(a)(2)(iii), 164.310(b), 164.310(c), 164.310(d)(1), 164.310(d)(2)(iii), 164.312(a), 164.312(b), 164.312e, 164.312(e)(2)(i), 164.314(a)(2)(i)(C), 164.314(a)(2)(iii), 164.314(b)(2)(i),	APO01.06, APO07.06, APO11.06, APO12.01, APO12.02, APO12.03, APO12.04, APO12.06, APO13.02, DSS02.07, DSS04.05, DSS05.07	#1: Inventory of Authorized and Unauthorized Devices #2: Inventory of Authorized and Unauthorized Software #3: Secure Configuration for End-User Devices #4: Continuous Vulnerability Assessment and Remediation #5: Controlled Use of Administrative Privileges #7: Email and Web Browser Protections #8: Malware Defenses #9: Limitation and Control of Network Ports #11: Secure Configurations for Network Devices #12: Boundary Defense #13: Data Protection #14: Controlled Access Based on the Need to Know #15: Wireless Access Control #16: Account Monitoring and Control	Shut down unnecessary services as each port, protocol, or service is a potential avenue for ingress into the network.

NIST Control ID	NIST Control Name	ISO 27001/2:2013	2016 SISM	FedRAMP	HIPAA Security Rule 45 C.F.R.	COBIT 5	CIS Critical Security Controls v6.1: 2016	FERPA Privacy Technical Assistance Center (PTAC) Data Security Checklist
SI-5	**Security Alerts, Advisories, and Directives**	A.6.1.3, A.6.1.4, A.12.5.1, A.16.1.2, A.16.1.3		SI-5 (a) SI-5 (c)	§§164.308(a)(1)(ii)(A) 164.308(a)(1)(ii)(D), 164.308(a)(3), 164.308(a)(4), 164.308(a)(5)(ii)(A), 164.308(a)(6), 164.308(a)(7)(ii)(E), 164.308(a)(8), 164.310(a)(1), 164.310(a)(2)(iii), 164.312(a)(1), 164.312(c), 164.312(e), 164.314, 164.316, 164.316(b)(2)(iii)	APO12.01, APO12.02, APO12.03, APO12.04		
SI-6	**Security Function Verification**		040511, 041104, 070202				#20: Penetration Tests and Red Team Exercises	
SI-7	**Software, Firmware, and Information Integrity**	A.12.2.1	040505, 040507, 040508		§§164.308(a)(1)(ii)(D), 164.312(b), 164.312(c)(1), 164.312(c)(2), 164.312(e)(2)(i)		#4: Continuous Vulnerability Assessment and Remediation	
SI-8	**Spam Protection**		030301, 030103				#8: Malware Defenses	
SI-9	**Information Input Restrictions**	**Withdrawn: Incorporated into AC-2, AC-3, AC-5, AC-6**						
SI-10	**Information Input Validation**		030202, 040701				#18: Application Software Security	
SI-11	**Error Handling**		040503				#18: Application Software Security	
SI-12	**Information Handling and Retention**	A.8.2.3, A.18.1.3, A.18.1.4, A.18.2.2	030301, 040701, 041201, 041204					
SI-13	**Predictable Failure Prevention**		041202, 070102, 070201					
SI-14	**Non-Persistence**							
SI-15	**Information Output Filtering**						#18: Application Software Security	
SI-16	**Memory Protection**						#18: Application Software Security	
SI-17	**Fail-Safe Procedures**		040509, 070103, 070201					