NIST Control ID (Rev. 5)	NIST Control Name (Rev. 5)	ISO 27001/2:2013	FedRAMP	HITRUST	HIPAA Security Rule 45 C.F.R.	CIS Critical Security Controls v8	FERPA Privacy Technical Assistance Center (PTAC) Data Security Checklist	SOC2
Access Control (AC)								
AC-1	**Access Control Policy and Procedures**	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, 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.18.2.2	AC-1 (b) (1) AC-1 (b) (2)	01.a Access Control Policy 01.i Policy on the Use of Network Services 01.v Information Access Restriction 04.a Information Security Policy Document 04.b Review of the Information Security Policy 05.a Management Commitment to Information Security 09.a Documented Operations Procedures 09.s Information Exchange Policies and Procedures	No Direct Mapping	CIS 6.1 - Establish an Access Granting Process	No Direct Mapping	CC5.2; CC5.3
AC-2	**Account Management**	A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.5, A.9.2.6	AC-2 (j)	01.a Access Control Policy 01.b User Registration 01.c Privilege Management 01.e Review of User Access Rights 01.j User Authentication for External Connections 01.w Sensitive System Isolation 02.i Removal of Access Rights	§§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)	CIS 6.1 - Establish an Access Granting Process CIS 6.2 - Establish an Access Revoking Process CIS 6.8 - Define and Maintain Role-Based Access Control	No Direct Mapping	CC6.1
AC-2 (1)	**Automated System Account Management**	No Direct Mapping	No Direct Mapping	01.b User Registration	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC6.1
AC-2 (2)	**Automated Temporary and Emergency Account**	No Direct Mapping	No Direct Mapping	01.b User Registration	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC6.1
AC-2 (3)	**Disable Accounts**	No Direct Mapping	No Direct Mapping	01.b User Registration	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC6.1
AC-2 (4)	**Automated Audit Actions**	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC7.2
AC-2 (5)	**Inactivity Logout**	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
AC-2 (13)	**Disable Accounts for High-Risk Individuals**	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
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.14.1.2, A.14.1.3, A.18.1.3	No Direct Mapping	01.c Privilege Management 01.s Use of System Utilities 01.v Information Access Restriction 09.q Information Handling Procedures 09.s Information Exchange Policies and Procedures 10.j Access Control to Program Source Code 10.k Change Control Procedures	§§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)	CIS 3.3 - Configure Data Access Control Lists CIS 6.7 - Centralize Access 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.	CC6.1

NIST Control ID (Rev. 5)	NIST Control Name (Rev. 5)	ISO 27001/2:2013	FedRAMP	HITRUST	HIPAA Security Rule 45 C.F.R.	CIS Critical Security Controls v8	FERPA Privacy Technical Assistance Center (PTAC) Data Security Checklist	SOC2
AC-4	**Information Flow Enforcement**	A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3	No Direct Mapping	01.m Segregation in Networks 01.o Network Routing Control 09.s Information Exchange Policies and Procedures	§§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), 164.312(c), 164.312(e)	No Direct Mapping	No Direct Mapping	CC6.7; CC6.1
AC-5	**Separation of Duties**	A.6.1.2	No Direct Mapping	01.a Access Control Policy 01.b User Registration 09.c Segregation of Duties	§§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	No Direct Mapping	No Direct Mapping	CC6.1
AC-6	**Least Privilege**	A.9.1.2, A.9.2.3, A.9.4.4, A.9.4.5	No Direct Mapping	01.c Privilege Management 01.i Policy on the Use of Network Services 01.s Use of System Utilities 01.v Information Access Restriction 01.y Teleworking 05.i Identification of Risks Related to External Parties 10.j Access Control to Program Source Code	§§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	No Direct Mapping	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).	CC6.1
AC-6 (1)	**Least Privilege – Authorize Access to Security Functions**	No Direct Mapping	No Direct Mapping	01.c Privilege Management 06.j Protection of Information Systems Audit Tools	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC6.3
AC-6 (2)	**Least Privilege | Non-Privileged Access for Nonsecurity Functions**	No Direct Mapping	No Direct Mapping	01.c Privilege Management 01.q User Identification and Authentication	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC6.3
AC-6 (7)	**Least Privilege | Review of User Privileges**	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
AC-6(9)	**Log Use of Privileged Functions**	No Direct Mapping	No Direct Mapping	01.c Privilege Management 09.aa Audit Logging	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC7.2
AC-7	**Unsuccessful Logon Attempts**	A.9.4.2	AC-7(a) AC-7(b)	01.p Secure Log-on Procedures	No Direct Mapping	CIS 4.10 - Enforce Automatic Device Lockout on Portable End-User Devices	No Direct Mapping	CC6.1
AC-8	**System Use Notification**	A.9.4.2	AC-8 (a) AC-8 (c)	01.p Secure Log-on Procedures 05.j Addressing Security When Dealing with Customers 06.e Prevention of Misuse of Information Assets 07.e Information Labeling and Handling	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC2.2
AC-9	**Previous Logon (Access) Notification**	A.9.4.2	No Direct Mapping	01.p Secure Log-on Procedures	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
AC-10	**Concurrent Session Control**	No Direct Mapping	No Direct Mapping	01.c Privilege Management 01.p Secure Log-on Procedures	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
AC-11	**Device Lock**	A.11.2.8, A.11.2.9	No Direct Mapping	01.g Unattended User Equipment 01.h Clear Desk and Clear Screen Policy 01.t Session Time-out	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC6.1
AC-11 (1)	**Device Lock – Pattern-Hiding Displays**	No Direct Mapping	No Direct Mapping	01.t Session Time-out	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC6.1
AC-12	**Session Termination**	No Direct Mapping	No Direct Mapping	01.t Session Time-out	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC6.1
AC-13	**Supervision and Review**	**Withdrawn: Incorporated into AC-2 and AU-6**						

NIST Control ID (Rev. 5)	NIST Control Name (Rev. 5)	ISO 27001/2:2013	FedRAMP	HITRUST	HIPAA Security Rule 45 C.F.R.	CIS Critical Security Controls v8	FERPA Privacy Technical Assistance Center (PTAC) Data Security Checklist	SOC2
AC-14	**Permitted Actions without Identification or Authentication**	No Direct Mapping	No Direct Mapping	01.v Information Access Restriction	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC6.1
AC-15	**Automated Marking**	**Withdrawn: Incorporated into MP-3**						
AC-16	**Security Attributes**	No Direct Mapping	No Direct Mapping	07.e Information Labeling and Handling	§§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)	No Direct Mapping	No Direct Mapping	No Direct Mapping
AC-17	**Remote Access | Managed Access Control Points**	A.6.2.1, A.6.2.2, A.13.1.1, A.13.2.1, A.14.1.2	No Direct Mapping	01.i Policy on the Use of Network Services 01.j User Authentication for External Connections 01.n Network Connection Control 01.y Teleworking 09.m Network Controls 09.s Information Exchange Policies and Procedures	§§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)	CIS 13.5 - Manage Access Control for Remote Assets	No Direct Mapping	CC6.6
AC-17 (1)	**Automated Monitoring / Control**	No Direct Mapping	No Direct Mapping	01.j User Authentication for External Connections	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC6.6
AC-17 (2)	**Protection of Confidentiality / Integrity Using Encryption**	No Direct Mapping	No Direct Mapping	01.j User Authentication for External Connections 01.y Teleworking 05.i Identification of Risks Related to External Parties 09.s Information Exchange Policies and Procedures	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC6.6
AC-17 (3)	**Remote Access – Managed Access Control Points**	No Direct Mapping	No Direct Mapping	01.n Network Connection Control	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC6.6
AC-17 (4)	**Remote Access – Privileged Commands and / Access**	No Direct Mapping	No Direct Mapping	01.j User Authentication for External Connections	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC6.6
AC-18	**Wireless Access**	A.6.2.1, A.13.1.1, A.13.2.1	No Direct Mapping	01.i Policy on the Use of Network Services 01.j User Authentication for External Connections 08.g Equipment Siting and Protection 09.m Network Controls	§§164.308(a)(1)(ii)(D) 164.312(a)(1), 164.312(b), 164.312(e)	CIS 4.2 - Establish and Maintain a Secure Configuration Process for Network Infrastructure CIS 12.6 - Use of Secure Network Management and Communication Protocols	No Direct Mapping	CC6.6
AC-18 (1)	**Wireless Access – Authentication and Encryption**	No Direct Mapping	No Direct Mapping	09.m Network Controls	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC6.6
AC-18 (3)	**Wireless Access | Disable Wireless Networking**	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
AC-19	**Access Control for Mobile Devices**	A.6.2.1, A.11.1.5, A.11.2.6, A.13.2.1	No Direct Mapping	01.x Mobile Computing and Communications	§§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)	CIS 6.4 - Require MFA for Remote Network Access	Mobile devices - Encrypt sensitive data are stored on mobile devices, such as laptops or smart phones.	CC6.6
AC-19 (5)	**Access Control for Mobile Devices – Full Device / Container-Based Encryption**	No Direct Mapping	No Direct Mapping	01.x Mobile Computing and Communications	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC6.6

NIST Control ID (Rev. 5)	NIST Control Name (Rev. 5)	ISO 27001/2:2013	FedRAMP	HITRUST	HIPAA Security Rule 45 C.F.R.	CIS Critical Security Controls v8	FERPA Privacy Technical Assistance Center (PTAC) Data Security Checklist	SOC2
AC-20	**Use of External Information Systems**	A.11.2.6, A.13.1.1, A.13.2.1	No Direct Mapping	01.i Policy on the Use of Network Services 01.y Teleworking 07.c Acceptable Use of Assets 08.k Security of Equipment Off-Premises 09.s Information Exchange Policies and Procedures	§§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)	CIS 15.3 - Classify Service Providers	No Direct Mapping	CC9.2
AC-20 (1)	**Use of External Information Systems – Limits on Authorized Use**	No Direct Mapping	No Direct Mapping	09.s Information Exchange Policies and Procedures	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC9.2
AC-20 (2)	**Use of External Information Systems – Portable Storage Devices**	No Direct Mapping	No Direct Mapping	09.s Information Exchange Policies and Procedures	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC6.7
AC-21	**Information Sharing**	No Direct Mapping	No Direct Mapping	01.b User Registration 01.c Privilege Management	§§164.308(a)(6)(ii)	No Direct Mapping	No Direct Mapping	CC6.3
AC-22	**Publicly Accessible Content**	No Direct Mapping	AC-22 (d)	09.z Publicly Available Information	No Direct Mapping	CIS 14.5 - Train Workforce Members on Causes of Unintentional Data Exposure	No Direct Mapping	CC6.3
AC-23	**Data Mining Protection**	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
AC-24	**Access Control Decisions**	A.9.4.1*	No Direct Mapping	No Direct Mapping	No Direct Mapping		No Direct Mapping	No Direct Mapping
AC-25	**Reference Monitor**	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
Awareness & Training (AT)								
AT-1	**Security Awareness and Training Policy and Procedures**	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2	AT-1 (b) (1) AT-1 (b) (2)	02.e Information Security Awareness, Education, and Training	No Direct Mapping	CIS 14.1 - Establish and Maintain a Security Awareness Program	Specify employee responsibilities associated with maintaining compliance with security policies	CC5.2
AT-2	**Literacy Training and Awareness**	7.3, A.7.2.2, A.12.2.1	AT-2(c)	01.p Secure Log-on Procedures	§§164.308(a)(5)	CIS 14.1 - Establish and Maintain a Security Awareness Program	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).	CC2.2
AT-2 (2)	**Literacy Training and Awareness-Insider Threat**	No Direct Mapping	No Direct Mapping	02.e Information Security Awareness, Education, and Training	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC2.2
AT-2 (3)	**Literacy Training and Awareness-Social Engineering and Mining**	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
AT-3	**Role Based Training**	A.7.2.2*	AT-3 ©	02.d Management Responsibilities	§§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)	CIS 14.9 - Conduct Role-Specific Security Awareness and Skills Training	No Direct Mapping	CC2.2
AT-4	**Training Records**	No Direct Mapping	AT-4 (b)	02.e Information Security Awareness, Education, and Training	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC2.2
AT-5	**Contacts with Security Groups and Associations**	**Withdrawn: Incorporated into PM-15**						
Audit & Accountability (AU)								

NIST Control ID (Rev. 5)	NIST Control Name (Rev. 5)	ISO 27001/2:2013	FedRAMP	HITRUST	HIPAA Security Rule 45 C.F.R.	CIS Critical Security Controls v8	FERPA Privacy Technical Assistance Center (PTAC) Data Security Checklist	SOC2
AU-1	**Audit and Accountability Policy and Procedures**	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2	AU-1 (b) (1) AU-1 (b) (2)	04.a Information Security Policy Document	§§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)	CIS 8.1 - Establish and Maintain an Audit Log Management Process	No Direct Mapping	CC5.2
AU-2	**Audit Events**	No Direct Mapping	AU-2 (a) AU-2 (d)	01.p Secure Log-on Procedures	§§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)	CIS 3.14 - Log Sensitive Data Access CIS 8.1 - Establish and Maintain an Audit Log Management Process CIS 8.2 - Collect Audit Logs	No Direct Mapping	CC7.2
AU-3	**Content of Audit Records**	A.12.4.1*	No Direct Mapping	09.aa Audit Logging	§§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)	CIS 8.5 - Collect Detailed Audit Logs	No Direct Mapping	CC7.2
AU-3 (1)	**Content of Audit Records - Additional Audit Information**	No Direct Mapping	No Direct Mapping	09.aa Audit Logging	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC7.2
AU-4	**Audit Storage Capacity**	A.12.1.3	No Direct Mapping	09.h Capacity Management	§§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)	CIS 8.3 - Ensure Adequate Audit Log Storage	No Direct Mapping	CC7.2
AU-5	**Response to Audit Processing Failures**	No Direct Mapping	AU-5(b)	09.aa Audit Logging	§§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)	No Direct Mapping	No Direct Mapping	CC7.2
AU-6	**Audit Review, Analysis, and Reporting**	A.12.4.1, A.16.1.2, A.16.1.4	AU-6(a)-1	01.b User Registration	§§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)	CIS 8.11 - Conduct Audit Log Reviews	No Direct Mapping	CC7.3
AU-6 (1)	**Audit Review, Analysis, and Reporting – Automated Process Integration**	No Direct Mapping	No Direct Mapping	09.ab Monitoring System Use	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC7.2
AU-6 (3)	**Audit Review, Analysis, and Reporting – Correlate Audit Repositories**	No Direct Mapping	No Direct Mapping	09.ab Monitoring System Use	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC7.2
AU-7	**Audit Reduction and Report Generation**	No Direct Mapping	No Direct Mapping	09.ab Monitoring System Use	§§164.308(a)(6)	No Direct Mapping	No Direct Mapping	CC7.3
AU-7 (1)	**Audit Reduction and Report Generation | Automatic Processing**	No Direct Mapping	No Direct Mapping	09.ab Monitoring System Use	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC7.3

NIST Control ID (Rev. 5)	NIST Control Name (Rev. 5)	ISO 27001/2:2013	FedRAMP	HITRUST	HIPAA Security Rule 45 C.F.R.	CIS Critical Security Controls v8	FERPA Privacy Technical Assistance Center (PTAC) Data Security Checklist	SOC2
AU-8	**Time Stamps**	A.12.4.4	No Direct Mapping	09.aa Audit Logging	§§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)	CIS 8.4 - Standardize Time Synchronization	No Direct Mapping	CC7.2
AU-8 (1)	**Time Stamps – Synchronization with Authoritative Time Source**	No Direct Mapping	No Direct Mapping	09.af Clock Synchronization	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC7.2
AU-9	**Protection of Audit Information**	A.12.4.2, A.12.4.3, A.18.1.3	No Direct Mapping	06.c Protection of Organizational Records	§§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)	No Direct Mapping	No Direct Mapping	CC7.2
AU-9 (4)	**Protection of Audit Information – Access by Subset of Privileged Users**	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC7.2
AU-10	**Non-repudiation**	No Direct Mapping	No Direct Mapping	09.x Electronic Commerce Services	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
AU-11	**Audit Record Retention**	A.12.4.1, A.16.1.7	AU-11	06.c Protection of Organizational Records	§§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)	CIS 8.10 - Retain Audit Logs	No Direct Mapping	CC7.2
AU-12	**Audit Generation**	A.12.4.1, A.12.4.3	AU-12 (a)	01.p Secure Log-on Procedures	§§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)	CIS 8.2 - Collect Audit Logs CIS 8.5 - Collect Detailed Audit Logs	No Direct Mapping	CC7.2
AU-13	**Monitoring for Information Disclosure**	No Direct Mapping	No Direct Mapping	No Direct Mapping	§§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)	No Direct Mapping	No Direct Mapping	No Direct Mapping
AU-14	**Session Audit**	A.12.4.1*	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
AU-15	**Alternate Audit Capability**	**Withdrawn: Incorporated into AU-5 (5)**						
AU-16	**Cross-Organizational Auditing**	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
Security Assessment & Authorization (CA)								
CA-1	**Security Assessment and Authorization Policies and Procedures**	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, 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)	04.a Information Security Policy Document	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC5.2

NIST Control ID (Rev. 5)	NIST Control Name (Rev. 5)	ISO 27001/2:2013	FedRAMP	HITRUST	HIPAA Security Rule 45 C.F.R.	CIS Critical Security Controls v8	FERPA Privacy Technical Assistance Center (PTAC) Data Security Checklist	SOC2
CA-2	**Control Assessments**	A.14.2.8, A.18.2.2, A.18.2.3	CA-2 (b) CA-2 (d) CA-2(1)	03.b Performing Risk Assessments	§§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)	No Direct Mapping	Audit and compliance monitoring - Conduct independent assessment of data protection capabilities and procedures	CC4.1
CA-2 (1)	**Control Assessments – Independent Assessors**	No Direct Mapping		05.a Management Commitment to Information Security	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC4.1
CA-3	**System Interconnections**	A.13.1.2, A.13.2.1, A.13.2.2	CA-3 ©	05.i Identification of Risks Related to External Parties	§§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)	No Direct Mapping	No Direct Mapping	CC6.6
CA-3 (5)	**Information Exchange – Restrictions on External System Connections**	**Withdrawn: Incorporated into SC-7 (5)**						
CA-4	**Security Certification**	**Withdrawn: Incorporated into CA-2**						No Direct Mapping
CA-5	**Plan of Action and Milestones**	8.3, 9.2, 10.1*	CA-5 CA-5(b)	03.c Risk Mitigation	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC4.2
CA-6	**Security Authorization**	9.3*	CA-6c CA-6 (c)	05.d Authorization Process for Information Assets and Facilities	§ 164.308(a)(4), 164.308(a)(3)), § 164.314(a)(1), § 164.312(a)(1)	No Direct Mapping	No Direct Mapping	CC8.1

NIST Control ID (Rev. 5)	NIST Control Name (Rev. 5)	ISO 27001/2:2013	FedRAMP	HITRUST	HIPAA Security Rule 45 C.F.R.	CIS Critical Security Controls v8	FERPA Privacy Technical Assistance Center (PTAC) Data Security Checklist	SOC2
CA-7	**Continuous Monitoring**	9.1, 9.2, A.18.2.2, A.18.2.3*	CA-7 CA-7 (g)	05.h Independent Review of Information Security	§§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), 164.314(a)(2)(iii),	CIS 3.13 - Deploy a Data Loss Prevention Solution CIS 13.1 - Centralize Security Event Alerting CSI 13.3 - Deploy a Network Intrusion Detection Solution	No Direct Mapping	CC4.1
CA-7 (1)	**Continuous Monitoring – Independent Assessment**	No Direct Mapping	No Direct Mapping	05.h Independent Review of Information Security	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC4.1
CA-7 (4)	**Continuous Monitoring – Risk Monitoring**	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
CA-8	**Penetration Testing**	No Direct Mapping	No Direct Mapping	10.m Control of Technical Vulnerabilities	§§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)	No Direct Mapping	No Direct Mapping	No Direct Mapping
CA-9	**Internal System Connections**	No Direct Mapping	No Direct Mapping	09.w Interconnected Business Information Systems	§§164.308(a)(1)(ii)(A) 164.308(a)(3)(ii)(A), 164.308(a)(8), 164.310(d)	CIS 4.4 - Implement and Manage a Firewall on Servers CIS 13.4 - Perform Traffic Filtering Between Network Segments	No Direct Mapping	CC8.1
Configuration Management (CM)								
CM-1	**Configuration Management Policy and Procedures**	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2	CM-1 (b) (1) CM-1 (b) (2)	04.a Information Security Policy Document	No Direct Mapping	CIS 4.1 - Establish and Maintain a Secure Configuration Process	No Direct Mapping	CC5.2
CM-2	**Baseline Configuration**	No Direct Mapping	No Direct Mapping	01.j User Authentication for External Connections	§§164.308(a)(1)(ii)(D), 164.308(a)(4), 164.312(b)	CIS 4.1 - Establish and Maintain a Secure Configuration Process	Network mapping - Capture network servers, routers, applications and associated data.	CC8.1
CM-2 (2)	**Baseline Configuration |Automation Support for Accuracy and Currency**	No Direct Mapping	No Direct Mapping	01.j User Authentication for External Connections	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
CM-2 (3)	**Baseline Configuration |Retention of previous configurations**	No Direct Mapping	No Direct Mapping	10.h Control of Operational Software	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC8.1
CM-2 (7)	**Baseline Configuration | Configure Systems and Components For High-Risk Areas**	No Direct Mapping	No Direct Mapping	01.x Mobile Computing and Communications	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC6.6

NIST Control ID (Rev. 5)	NIST Control Name (Rev. 5)	ISO 27001/2:2013	FedRAMP	HITRUST	HIPAA Security Rule 45 C.F.R.	CIS Critical Security Controls v8	FERPA Privacy Technical Assistance Center (PTAC) Data Security Checklist	SOC2
CM-3	**Configuration Change Control**	8.1, A.12.1.2, A.14.2.2, A.14.2.3, A.14.2.4	No Direct Mapping	03.d Risk Evaluation	§§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),	No Direct Mapping	Change management - Analyze and address security and privacy risks introduced by new technology or business processes.	CC8.1
CM-3 (4)	**Configuration Change Control | Security and Privacy Representatives**	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
CM-4	**Security Impact Analysis**	A.14.2.3	No Direct Mapping	09.b Change Management	§§164.308(a)(4), 164.308(a)(8), 164.308(a)(7)(i), 164.308(a)(7)(ii)	No Direct Mapping	No Direct Mapping	CC8.1
CM-4 (2)		No Direct Mapping	No Direct Mapping	10.k Change Control Procedures	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
CM-5	**Access Restrictions for Change**	A.9.2.3, A.9.4.5, A.12.1.2, A.12.1.4, A.12.5.1	No Direct Mapping	09.b Change Management	§§164.308(a)(8), 164.308(a)(7)(i), 164.308(a)(7)(ii)	No Direct Mapping	No Direct Mapping	CC8.1
CM-6	**Configuration Settings**	No Direct Mapping	CM-6 (a)	09.z Publicly Available Information	§§164.308(a)(8), 164.308(a)(7)(i), 164.308(a)(7)(ii)	CIS 4.1 - Establish and Maintain a Secure Configuration Process	Secure configurations - Security test hardware and software configurations to optimize its security.	CC6.1
CM-7	**Least Functionality**	A.12.5.1*	CM-7 CM-7 (b)	01.c Privilege Management	§§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)	CIS 4.1 - Establish and Maintain a Secure Configuration Process CIS 12.2 - Establish and Maintain a Secure Network Architecture	No Direct Mapping	CC6.1
CM-7 (1)	**Least Functionality | Periodic Review**	No Direct Mapping	No Direct Mapping	01.l Remote Diagnostic and Configuration Port Protection	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC6.1
CM-7 (2)	**Least Functionality | Prevent Program Execution**	No Direct Mapping	No Direct Mapping	01.l Remote Diagnostic and Configuration Port Protection	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC6.1
CM-7 (5)	**Least Functionality | Authorized Software**	No Direct Mapping	No Direct Mapping	01.l Remote Diagnostic and Configuration Port Protection	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping

NIST Control ID (Rev. 5)	NIST Control Name (Rev. 5)	ISO 27001/2:2013	FedRAMP	HITRUST	HIPAA Security Rule 45 C.F.R.	CIS Critical Security Controls v8	FERPA Privacy Technical Assistance Center (PTAC) Data Security Checklist	SOC2
CM-8	**Information System Component Inventory**	A.8.1.1, A.8.1.2	CM-8 CM-8 (b)	07.a Inventory of Assets	§§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)	CIS 1.1 - Establish and Maintain Detailed Enterprise Asset Inventory CIS 2.1 - Establish and Maintain a Software Inventory	Inventory of assets - Include both authorized and unauthorized devices used in the computing environment.	CC6.1
CM-8 (1)	**System Component Inventory | Updates during Installation and Removal**	No Direct Mapping	No Direct Mapping	07.a Inventory of Assets	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC6.1
CM-8 (3)	**System Component Inventory – Automated Unauthorized Component Detection**	No Direct Mapping	No Direct Mapping	07.a Inventory of Assets	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC6.1
CM-9	**Configuration Management Plan**	A.6.1.1*	No Direct Mapping	09.b Change Management	§§164.308(a)(8), 164.308(a)(7)(i), 164.308(a)(7)(ii)	No Direct Mapping	No Direct Mapping	CC8.1
CM-10	**Software Usage Restrictions**	A.18.1.2	No Direct Mapping	06.b Intellectual Property Rights	§§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)	CIS 2.5 - Allowlist Authorized Software	No Direct Mapping	CC6.8
CM-11	**User-Installed Software**	A.12.5.1, A.12.6.2	CM-11	09.j Controls Against Malicious Code	§§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)	CIS 2.3 - Address Unauthorized Software	No Direct Mapping	CC6.8
Contingency Planning (CP)								
CP-1	**Contingency Planning Policy and Procedures**	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2	CP-1 (b)(1) CP-1 (b)(2)	04.a Information Security Policy Document	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC9.1

NIST Control ID (Rev. 5)	NIST Control Name (Rev. 5)	ISO 27001/2:2013	FedRAMP	HITRUST	HIPAA Security Rule 45 C.F.R.	CIS Critical Security Controls v8	FERPA Privacy Technical Assistance Center (PTAC) Data Security Checklist	SOC2
CP-2	**Contingency Plan**	7.5.1, 7.5.2, 7.5.3, A.6.1.1, A.17.1.1, A.17.2.1	CP-2 CP-2 (d)	05.f Contact with Authorities	§§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)	No Direct Mapping	No Direct Mapping	CC9.1
CP-3	**Contingency Training**	A.7.2.2*	CP-3 (a) CP-3 (c)	02.e Information Security Awareness, Education, and Training	§§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)	No Direct Mapping	No Direct Mapping	CC9.1
CP-4	**Contingency Plan Testing**	A.17.1.3	CP-4(a) CP-4 (a)-1 CP-4 (a)-2	02.e Information Security Awareness, Education, and Training	§§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)	CIS 11.5 - Test Data Recovery	No Direct Mapping	A1.3
CP-5	**Contingency Plan Update**	**Withdrawn: Incorporated into CP-2**						No Direct Mapping
CP-6	**Alternate Storage Site**	A.11.1.4, A.17.1.2, A.17.2.1	No Direct Mapping	09.l Back-up	§§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)	No Direct Mapping	No Direct Mapping	A1.2; CC7.5
CP-7	**Alternate Processing Site**	A.11.1.4, A.17.1.2, A.17.2.1	No Direct Mapping	12.c Developing and Implementing Continuity Plans Including Information Security	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC9.1; CC7.5
CP-8	**Telecommunications Services**	A.11.2.2, A.17.1.2	No Direct Mapping	08.h Supporting Utilities	§§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)	No Direct Mapping	No Direct Mapping	CC9.1
CP-9	**Information System Backup**	A.12.3.1, A.17.1.2, A.18.1.3	CP-9 CP-9 (a) CP-9 (b) CP-9 (c)	09.l Back-up	§§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)	CIS 11.2 - Perform Automated Backups CIS 11.3 - Protect Recovery Data	No Direct Mapping	A1.2
CP-9 (1)	**Information System Backup – Testing for Reliability/Integrity**	No Direct Mapping	No Direct Mapping	09.l Back-up	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping

NIST Control ID (Rev. 5)	NIST Control Name (Rev. 5)	ISO 27001/2:2013	FedRAMP	HITRUST	HIPAA Security Rule 45 C.F.R.	CIS Critical Security Controls v8	FERPA Privacy Technical Assistance Center (PTAC) Data Security Checklist	SOC2
CP-9 (8)	**System Backup | Cryptographic Protection**	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
CP-10	**Information System Recovery and Reconstitution**	A.17.1.2	No Direct Mapping	No Direct Mapping	§§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)	CIS 11.2 - Perform Automated Backups	No Direct Mapping	CC9.1; CC7.5
CP-11	**Alternate Communications Protocols**	A.17.1.2*	No Direct Mapping	12.c Developing and Implementing Continuity Plans Including Information Security	§§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)	No Direct Mapping	No Direct Mapping	No Direct Mapping
CP-12	**Safe Mode**	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
CP-13	**Alternative Security Mechanisms**	A.17.1.2*	No Direct Mapping	No Direct Mapping	No Direct Mapping		No Direct Mapping	No Direct Mapping
Identification & Authentication (IA)								
IA-1	**Identification and Authentication Policy and Procedures**	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2	IA-1 (b) (1) IA-1 (b) (2)	01.b User Registration	§§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)	No Direct Mapping	No Direct Mapping	CC5.2
IA-2	**Identification and Authentication (Organizational Users)**	A.9.2.1	IA-2 (12)	01.d User Password Management	§§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)	No Direct Mapping	Authentication - Consider TFA for remote users or privileged “super users.”	CC6.1
IA-2 (1)	**Identification and Authentication (Organizational Users) | Multi-factor Authentication to Privileged Accounts**	No Direct Mapping	No Direct Mapping	01.q User Identification and Authentication	No Direct Mapping	CIS 6.5 - Require MFA for Administrative Access	No Direct Mapping	CC6.1
IA-2 (2)	**Identification and Authentication (Organizational Users) | Multi-factor Authentication to Non-Privileged Accounts**	No Direct Mapping	No Direct Mapping	01.q User Identification and Authentication	No Direct Mapping	CIS 6.3 - Require MFA for Externally-Exposed Applications CIS 6.4 - Require MFA for Remote Network Access	No Direct Mapping	CC6.1
IA-2 (8)	**Identification and Authentication (Organizational Users) | Access to Accounts – Replay Resistant**	No Direct Mapping	No Direct Mapping	01.q User Identification and Authentication	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC6.1
IA-2 (12)	**Identification and Authentication (Organizational Users) | Acceptance of PIV Credentials**	No Direct Mapping	No Direct Mapping	01.q User Identification and Authentication	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC6.1
IA-3	**Device Identification and Authentication**	No Direct Mapping	No Direct Mapping	01.j User Authentication for External Connections	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC6.1
IA-4	**Identifier Management**	A.9.2.1	IA-4 (d) IA-4 (e)	01.b User Registration	§§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)	CIS 5.1 - Establish and Maintain an Inventory of Accounts CIS 6.1 - Establish an Access Granting Process	No Direct Mapping	CC6.2

NIST Control ID (Rev. 5)	NIST Control Name (Rev. 5)	ISO 27001/2:2013	FedRAMP	HITRUST	HIPAA Security Rule 45 C.F.R.	CIS Critical Security Controls v8	FERPA Privacy Technical Assistance Center (PTAC) Data Security Checklist	SOC2
IA-4 (5)	**Identifier Management | Identify User Status**	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
IA-5	**Authenticator Management**	A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.3	IA-5 (1) (a) IA-5 (1) (b) IA-5 (1) (d) IA-5 (1) (e) IA-5 (g)	01.b User Registration	§§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)	CIS 3.10 - Encrypt Sensitive Data in Transit CIS 4.1 - Establish and Maintain a Secure Configuration Process CIS 4.7 - Manage Default Accounts on Enterprise Assets and Software CIS 6.1 - Establish an Access Granting Process	No Direct Mapping	CC6.2
IA-5 (1)	**Authenticator Management | Password-based authentication**	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	CIS 3.10 - Encrypt Sensitive Data in Transit CIS 3.11 - Encrypt Sensitive Data at Rest CIS 5.2 - Use Unique Passwords	No Direct Mapping	CC6.2
IA-5 (6)	**Authenticator Management | Protection of Authenticators**	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
IA-6	**Authenticator Feedback**	A.9.4.2	No Direct Mapping	01.d User Password Management	§§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)	No Direct Mapping	No Direct Mapping	CC6.1
IA-7	**Cryptographic Module Authentication**	A.18.1.5	No Direct Mapping	06.f Regulation of Cryptographic Controls	§§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)	No Direct Mapping	No Direct Mapping	CC6.1
IA-8	**Identification and Authentication (Non-Organizational Users)**	A.9.2.1	No Direct Mapping	01.j User Authentication for External Connections	§§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)	No Direct Mapping	No Direct Mapping	CC6.1
IA-8 (1)	**Identification and Authentication (Non-Organizational Users) | Acceptance of PIV Credentials From Other Agencies**	No Direct Mapping	No Direct Mapping	01.j User Authentication for External Connections	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC6.1
IA-8 (2)	**Identification and Authentication (Non-Organizational Users) | Acceptance of External Authenticators**	No Direct Mapping	No Direct Mapping	01.j User Authentication for External Connections	No Direct Mapping	CIS 6.6 - Establish and Maintain an Inventory of Authentication and Authorization Systems	No Direct Mapping	CC6.1
IA-8 (4)	**Identification and Authentication (Non-Organizational Users) | Use of Defined Profiles**	No Direct Mapping	No Direct Mapping	01.j User Authentication for External Connections	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC6.1

NIST Control ID (Rev. 5)	NIST Control Name (Rev. 5)	ISO 27001/2:2013	FedRAMP	HITRUST	HIPAA Security Rule 45 C.F.R.	CIS Critical Security Controls v8	FERPA Privacy Technical Assistance Center (PTAC) Data Security Checklist	SOC2
IA-9	**Service Identification and Authentication**	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
IA-10	**Adaptive Identification and Authentication**	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
IA-11	**Re-authentication**	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
IA-12	**Identity Proofing**	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
IA-12 (2)	**Identity Proofing |Identity Evidence**	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
IA-12 (3)	**Identity Proofing | Identity Evidence Validation and Verification**	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
IA-12 (5)	**Identity Proofing | Address Confirmation**	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
				Incident Response (IR)				
IR-1	**Incident Response Policy and Procedures**	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1 A.18.1.1, A.18.2.2	IR-1 (b) (1) IR-1 (b) (2)	04.a Information Security Policy Document	No Direct Mapping	CIS 17.1 - Designate Personnel to Manage Incident Handling CIS 17.4 - Establish and Maintain an Incident Response Process CIS 17.5 - Assign Key Roles and Responsibilities	No Direct Mapping	CC5.2
IR-2	**Incident Response Training**	A.7.2.2*	IR-2 (c)	02.e Information Security Awareness, Education, and Training	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC7.4
IR-3	**Incident Response Testing**	No Direct Mapping	No Direct Mapping	11.c Responsibilities and Procedures	§§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),16 4.310(a)(2)(i), 164.308(a)(6)(i), 164.312(a)(2)(ii)	No Direct Mapping	No Direct Mapping	CC7.4
IR-3 (2)	**Incident Response Plan Testing – Coordination With Related Plans**	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC7.4
IR-4	**Incident Handling**	A.16.1.4, A.16.1.5, A.16.1.6	IR-4	05.b Information Security Coordination	§§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)	CIS 17.8 - Conduct Post-Incident Reviews	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.	CC7.4
IR-4 (1)	**Incident Handling – Automated Incident Handling Process**	No Direct Mapping	No Direct Mapping	11.a Reporting Information Security Events	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC7.4

NIST Control ID (Rev. 5)	NIST Control Name (Rev. 5)	ISO 27001/2:2013	FedRAMP	HITRUST	HIPAA Security Rule 45 C.F.R.	CIS Critical Security Controls v8	FERPA Privacy Technical Assistance Center (PTAC) Data Security Checklist	SOC2
IR-5	**Incident Monitoring**	No Direct Mapping	No Direct Mapping	02.f Disciplinary Process	§§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)	CIS 17.3 - Establish and Maintain an Enterprise Process for Reporting Incidents	No Direct Mapping	CC7.4
IR-6	**Incident Reporting**	A.6.1.3, A.16.1.2	IR-6 (a)	05.f Contact with Authorities	§§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)	CIS 17.2 - Establish and Maintain Contact Information for Reporting Security Incidents CIS 17.3 - Establish and Maintain an Enterprise Process for Reporting Incidents	No Direct Mapping	CC7.2
IR-6 (1)	**Incident Reporting – Automated Reporting**	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC7.2
IR-6 (3)	**Incident Reporting – Supply Chain**	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
IR-7	**Incident Response Assistance**	No Direct Mapping	No Direct Mapping	11.c Responsibilities and Procedures	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC7.4
IR-7 (1)	**Incident Response Assistance – Automation Support for Availability of Information and Support**	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC7.4
IR-8	**Incident Response Plan**	7.5.1, 7.5.2, 7.5.3, A.16.1.1	IR-8 (b) IR-8 (c) IR-8 (e)	11.c Responsibilities and Procedures	§§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)	CIS 17.1 - Designate Personnel to Manage Incident Handling CIS 17.4 - Establish and Maintain an Incident Response Process CIS 17.5 - Assign Key Roles and Responsibilities CIS 17.9 - Establish and Maintain Security Incident Thresholds	No Direct Mapping	CC7.4
IR-9	**Information Spillage Response**	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
IR-10	**Integrated Information Security Analysis Team**	**Withdrawn: Incorporated into IR-4 (11)**						No Direct Mapping
Maintenance (MA)								
MA-1	**System Maintenance Policy and Procedures**	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2	MA-1 (b) (1) MA-1 (b) (2)	04.a Information Security Policy Document	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC5.2
MA-2	**Controlled Maintenance**	A.11.2.4*, A.11.2.5*	No Direct Mapping	08.a Physical Security Perimeter	§§164.308(a)(3)(ii)(A) 164.310(a)(2)(iv)	No Direct Mapping	No Direct Mapping	CC8.1
MA-3	**Maintenance Tools**	No Direct Mapping	No Direct Mapping	08.j Equipment Maintenance	§§164.308(a)(3)(ii)(A) 164.310(a)(2)(iv)	No Direct Mapping	No Direct Mapping	CC8.1
MA-3 (1)	**Maintenance Tools - Inspect Tools**	No Direct Mapping	No Direct Mapping	08.j Equipment Maintenance	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC8.1
MA-3 (2)	**Maintenance Tools - Inspect Media**	No Direct Mapping	No Direct Mapping	08.j Equipment Maintenance	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC6.8
MA-3 (3)	**Maintenance Tools – Prevent Unauthorized Removal**	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping

NIST Control ID (Rev. 5)	NIST Control Name (Rev. 5)	ISO 27001/2:2013	FedRAMP	HITRUST	HIPAA Security Rule 45 C.F.R.	CIS Critical Security Controls v8	FERPA Privacy Technical Assistance Center (PTAC) Data Security Checklist	SOC2
MA-4	**Nonlocal Maintenance**	No Direct Mapping	No Direct Mapping	01.j User Authentication for External Connections	§§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)	No Direct Mapping	No Direct Mapping	CC6.6
MA-4 (2)	**Nonlocal Maintenance – Document Nonlocal Maintenance**	No Direct Mapping	No Direct Mapping	01.l Remote Diagnostic and Configuration Port Protection	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC8.1
MA-5	**Maintenance Personnel**	No Direct Mapping	No Direct Mapping	08.j Equipment Maintenance	§§164.308(a)(3)(ii)(A) 164.310(a)(2)(iv)	No Direct Mapping	No Direct Mapping	CC1.4
MA-6	**Timely Maintenance**	A.11.2.4	No Direct Mapping	08.j Equipment Maintenance	No Direct Mapping	No Direct Mapping	No Direct Mapping	A1.2
Media Protection (MP)								
MP-1	**Media Protection Policy and Procedures**	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2	MP-1 (b) (1) MP-1 (b) (2)	01.a Access Control Policy	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC5.2
MP-2	**Media Access**	A.8.2.3, A.8.3.1, A.11.2.9	No Direct Mapping	09.q Information Handling Procedures	§§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)	CIS 3.3 - Configure Data Access Control Lists	No Direct Mapping	CC6.4
MP-3	**Media Marking**	A.8.2.2	No Direct Mapping	01.h Clear Desk and Clear Screen Policy	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC6.7
MP-4	**Media Storage**	A.8.2.3, A.8.3.1, A.11.2.9	No Direct Mapping	01.h Clear Desk and Clear Screen Policy	§§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)	No Direct Mapping	No Direct Mapping	CC6.5
MP-5	**Media Transport**	A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.5, A.11.2.6	No Direct Mapping	08.k Security of Equipment Off-Premises	§§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)	No Direct Mapping	No Direct Mapping	CC6.7
MP-6	**Media Sanitization**	A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7	No Direct Mapping	08.l Secure Disposal or Re-Use of Equipment	§§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)	CIS 3.5 - Securely Dispose of Data	No Direct Mapping	CC6.5
MP-7	**Media Use**	A.8.2.3, A.8.3.1	No Direct Mapping	09.o Management of Removable Media	§§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)	CSI 3.9 - Encrypt Data on Removable Media	No Direct Mapping	CC6.7
MP-7 (1)	**Media Use – Prohibit Use Without Owner**	No Direct Mapping	No Direct Mapping	09.o Management of Removable Media	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC6.7
MP-8	**Media Downgrading**	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
Physical & Environmental Protection PE)								

NIST Control ID (Rev. 5)	NIST Control Name (Rev. 5)	ISO 27001/2:2013	FedRAMP	HITRUST	HIPAA Security Rule 45 C.F.R.	CIS Critical Security Controls v8	FERPA Privacy Technical Assistance Center (PTAC) Data Security Checklist	SOC2
PE-1	**Physical and Environmental Protection Policy and Procedures**	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2	PE-1 (b) (1) PE-1 (b) (2)	04.a Information Security Policy Document	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC5.2
PE-2	**Physical Access Authorizations**	A.11.1.2*	PE-2	08.b Physical Entry Controls	§§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)	No Direct Mapping	No Direct Mapping	CC6.4
PE-3	**Physical Access Control**	A.11.1.1, A.11.1.2, A.11.1.3	PE-3 (a) (2) PE-3 (d) PE-3 (f) PE-3 (g)	08.a Physical Security Perimeter	§§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)	No Direct Mapping	Make computing resources physically unavailable to unauthorized users. This includes securing access to any areas where sensitive data are stored and processed.	CC6.4
PE-4	**Access Control for Transmission Medium**	A.11.1.2, A.11.2.3	No Direct Mapping	08.i Cabling Security	§§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)	No Direct Mapping	No Direct Mapping	CC6.4
PE-5	**Access Control for Output Devices**	A.11.1.2, A.11.1.3	No Direct Mapping	01.g Unattended User Equipment	§§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)	No Direct Mapping	No Direct Mapping	CC6.4

NIST Control ID (Rev. 5)	NIST Control Name (Rev. 5)	ISO 27001/2:2013	FedRAMP	HITRUST	HIPAA Security Rule 45 C.F.R.	CIS Critical Security Controls v8	FERPA Privacy Technical Assistance Center (PTAC) Data Security Checklist	SOC2
PE-6	**Monitoring Physical Access**	No Direct Mapping	PE-6 (b)	08.b Physical Entry Controls	§§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)	No Direct Mapping	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).	CC6.4
PE-6 (1)	**Monitoring Physical Access – Intrusion Alarms / Surveillance Equipment**	No Direct Mapping	No Direct Mapping	08.b Physical Entry Controls	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC6.4
PE-7	**Visitor Control**	**Withdrawn: Incorporated into PE-2 and PE-3**						No Direct Mapping
PE-8	**Visitor Access Records**	No Direct Mapping	PE-8 (a) PE-8 (b)	08.b Physical Entry Controls	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC6.4
PE-9	**Power Equipment and Cabling**	A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3	No Direct Mapping	08.h Supporting Utilities	§§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), 164.314(b)(2)(i)	No Direct Mapping	No Direct Mapping	A1.2
PE-10	**Emergency Shutoff**	A.11.2.2*	No Direct Mapping	08.h Supporting Utilities	§§164.308(a)(7)(i), 164.308(a)(7)(ii)(C), 164.310, 164.316(b)(2)(iii)	No Direct Mapping	No Direct Mapping	A1.2
PE-11	**Emergency Power**	A.11.2.2	No Direct Mapping	08.h Supporting Utilities	§§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)	No Direct Mapping	No Direct Mapping	A1.2
PE-12	**Emergency Lighting**	A.11.2.2*	No Direct Mapping	08.h Supporting Utilities	§§164.308(a)(7)(i), 164.308(a)(7)(ii)(C), 164.310, 164.316(b)(2)(iii)	No Direct Mapping	No Direct Mapping	A1.2
PE-13	**Fire Protection**	A.11.1.4, A.11.2.1	No Direct Mapping	08.d Protecting Against External and Environmental Threats	§§164.308(a)(7)(i), 164.308(a)(7)(ii)(C), 164.310, 164.316(b)(2)(iii)	No Direct Mapping	No Direct Mapping	A1.2
PE-13 (1)	**Fire Protection – Detection Systems - Automatic Activation and Notification**	No Direct Mapping	No Direct Mapping	08.d Protecting Against External and Environmental Threats	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
PE-14	**Temperature and Humidity Controls**	A.11.1.4, A.11.2.1, A.11.2.2	PE-14 (a) PE-14 (b)	08.g Equipment Siting and Protection	§§164.308(a)(7)(i), 164.308(a)(7)(ii)(C), 164.310, 164.316(b)(2)(iii)	No Direct Mapping	No Direct Mapping	A1.2

NIST Control ID (Rev. 5)	NIST Control Name (Rev. 5)	ISO 27001/2:2013	FedRAMP	HITRUST	HIPAA Security Rule 45 C.F.R.	CIS Critical Security Controls v8	FERPA Privacy Technical Assistance Center (PTAC) Data Security Checklist	SOC2
PE-15	**Water Damage Protection**	A.11.1.4, A.11.2.1, A.11.2.2	No Direct Mapping	08.d Protecting Against External and Environmental Threats	§§164.308(a)(7)(i), 164.308(a)(7)(ii)(C), 164.310, 164.316(b)(2)(iii)	No Direct Mapping	No Direct Mapping	A1.2
PE-16	**Delivery and Removal**	A.8.2.3, A.11.1.6, A.11.2.5	PE-16	08.f Public Access, Delivery, and Loading Areas	§§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)	No Direct Mapping	No Direct Mapping	CC6.4
PE-17	**Alternate Work Site**	A.6.2.2, A.11.2.6, A.13.2.1	No Direct Mapping	01.y Teleworking	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC6.4
PE-18	**Location of Information System Components**	A.8.2.3, A.11.1.4, A.11.2.1	No Direct Mapping	01.g Unattended User Equipment	§§164.308(a)(7)(i), 164.308(a)(7)(ii)(C), 164.310, 164.316(b)(2)(iii)	No Direct Mapping	No Direct Mapping	No Direct Mapping
PE-19	**Information Leakage**	A.11.1.4, A.11.2.1	No Direct Mapping	No Direct Mapping	§§164.308(a)(1)(ii)(D), 164.308(a)(3), 164.308(a)(4), 164.310(b), 164.310(c), 164.312(a), 164.312(e)	No Direct Mapping	No Direct Mapping	No Direct Mapping
PE-20	**Asset Monitoring and Tracking**	A.8.2.3*	No Direct Mapping	No Direct Mapping	§§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)	No Direct Mapping	No Direct Mapping	No Direct Mapping
				Planning (PL)				
PL-1	**Security Planning Policy and Procedures**	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, 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)	04.a Information Security Policy Document	No Direct Mapping	No Direct Mapping	Policy and governance - organizational policies and standards regarding data security and individual privacy protection	CC5.2
PL-2	**System Security Plan**	7.5.1, 7.5.2, 7.5.3, 10.1, A.14.1.1	PL-2 (c)	05.b Information Security Coordination	§§164.306(e), 164.308(a)(7)(ii)(D), 164.308(a)(8), 164.316(b)(2)(iii)	No Direct Mapping	No Direct Mapping	CC5.3
PL-3	**System Security Plan Update**	**Withdrawn: Incorporated into PL-2**						No Direct Mapping
PL-4	**Rules of Behavior**	A.7.1.2, A.7.2.1, A.8.1.3	PL-4 (c)	01.y Teleworking	No Direct Mapping	No Direct Mapping	Personnel security - policies and guidelines concerning personal and work-related use of Internet, Intranet, and extranet systems	CC2.2
PL-4 (1)	**Rules of Behavior – Social Media and External Site/ Application Usage Restrictions**	No Direct Mapping	No Direct Mapping	07.c Acceptable Use of Assets	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC2.2
PL-5	**Privacy Impact Assessment**	**Withdrawn: Incorporated into Appendix J, AR-2, RA-3**						No Direct Mapping
PL-6	**Security Related Activity Planning**	**Withdrawn: Incorporated into PL-2**						No Direct Mapping
PL-7	**Security Concept of Operations**	8.1, A.14.1.1	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
PL-8	**Information Security Architecture**	A.14.1.1*	No Direct Mapping	10.a Security Requirements Analysis and Specification	§§164.308(a)(1)(i), 164.308(a)(1)(ii)(A), 164.308(a)(3)(ii)(A), 164.308(a)(8), 164.310(d)	No Direct Mapping	No Direct Mapping	CC5.2
PL-9	**Central Management**	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
PL-10	**Baseline Selection**	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping

NIST Control ID (Rev. 5)	NIST Control Name (Rev. 5)	ISO 27001/2:2013	FedRAMP	HITRUST	HIPAA Security Rule 45 C.F.R.	CIS Critical Security Controls v8	FERPA Privacy Technical Assistance Center (PTAC) Data Security Checklist	SOC2
PL-11	**Baseline Tailoring**	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
				Program Management (PM)				
PM-1	**Information Security Program Plan**	4.1, 4.2, 4.3, 4.4, 5.2, 5.3, 6.1.1, 6.2, 7.4, 7.5.1, 7.5.2, 7.5.3, 8.1, 9.3, 10.2, A.5.1.1, A.5.1.2, A.6.1.1, A.18.1.1, A.18.2.2	No Direct Mapping	00.a Information Security Management Program	§§164.308(a)(1)(i), 164.308(a)(2), 164.308(a)(3), 164.308(a)(4), 164.314, 164.316	No Direct Mapping	No Direct Mapping	No Direct Mapping
PM-2	**Senior Information Security Officer**	5.1, 5.3, A.6.1.1	No Direct Mapping	00.a Information Security Management Program	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
PM-3	**Information Security Resources**	5.1, 6.2, 7.1	No Direct Mapping	00.a Information Security Management Program	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
PM-4	**Plan of Action and Milestones Process**	6.1.1, 6.2, 7.5.1, 7.5.2, 7.5.3, 8.3, 9.2, 9.3, 10.1	No Direct Mapping	00.a Information Security Management Program	§§164.308(a)(1)(ii)(B), 164.314(a)(2)(i)(C), 164.314(b)(2)(iv)	No Direct Mapping	No Direct Mapping	No Direct Mapping
PM-5	**Information System Inventory**	No Direct Mapping	No Direct Mapping	07.a Inventory of Assets	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
PM-6	**Information Security Measures of Performance**	5.3, 6.1.1, 6.2, 9.1,	No Direct Mapping	00.a Information Security Management Program	§§164.306(e), 164.308(a)(7)(ii)(D), 164.308(a)(8), 164.316(b)(2)(iii)	No Direct Mapping	No Direct Mapping	No Direct Mapping
PM-7	**Enterprise Architecture**	No Direct Mapping	No Direct Mapping	10.a Security Requirements Analysis and Specification	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
PM-8	**Critical Infrastructure Plan**	No Direct Mapping	No Direct Mapping	12.b Business Continuity and Risk Assessment	§§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	No Direct Mapping	Layered defense - Protect hosts (individual computers), application, network, and perimeter.	No Direct Mapping
PM-9	**Risk Management Strategy**	4.3, 4.4, 6.1.1, 6.1.2, 6.2, 7.5.1, 7.5.2, 7.5.3, 9.3, 10.2	No Direct Mapping	00.a Information Security Management Program	§§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)	No Direct Mapping	No Direct Mapping	No Direct Mapping
PM-10	**Security Authorization Process**	9.3, A.6.1.1*	No Direct Mapping	05.c Allocation of Information Security Responsibilities	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
PM-11	**Mission/Business Process Definition**	4.1	No Direct Mapping	03.a Risk Management Program Development	§§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)	No Direct Mapping	No Direct Mapping	No Direct Mapping

NIST Control ID (Rev. 5)	NIST Control Name (Rev. 5)	ISO 27001/2:2013	FedRAMP	HITRUST	HIPAA Security Rule 45 C.F.R.	CIS Critical Security Controls v8	FERPA Privacy Technical Assistance Center (PTAC) Data Security Checklist	SOC2
PM-12	**Insider Threat Program**	No Direct Mapping	No Direct Mapping	11.a Reporting Information Security Events	§§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	No Direct Mapping	No Direct Mapping	No Direct Mapping
PM-13	**Information Security Workforce**	7.2, A.7.2.2*	No Direct Mapping	00.a Information Security Management Program	§§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)	#17: Security Skills Assessment and Appropriate Training	No Direct Mapping	No Direct Mapping
PM-14	**Testing, Training, and Monitoring**	6.2*	No Direct Mapping	02.d Management Responsibilities	§§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)	No Direct Mapping	No Direct Mapping	No Direct Mapping
PM-15	**Contacts with Security Groups and Associations**	7.4, A.6.1.4	No Direct Mapping	02.d Management Responsibilities	§§164.308(a)(6), 164.308(a)(7)(i), 164.308(a)(7)(ii)(C), 164.310, 164.316(b)(2)(iii)	No Direct Mapping	No Direct Mapping	No Direct Mapping
PM-16	**Threat Awareness Program**	No Direct Mapping	No Direct Mapping	No Direct Mapping	§§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)	No Direct Mapping	No Direct Mapping	No Direct Mapping
Personnel Security (PS)								
PS-1	**Personnel Security Policy and Procedures**	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2	PS-1 (b) (1) PS-1 (b) (2)	02.a Roles and Responsibilities	§§164.308(a)(1)(ii)(C), 164.308(a)(3)	No Direct Mapping	No Direct Mapping	CC5.2
PS-2	**Position Risk Designation**	No Direct Mapping	PS-2 (c)	02.a Roles and Responsibilities	§§164.308(a)(1)(ii)(C), 164.308(a)(3)	No Direct Mapping	No Direct Mapping	CC1.4

NIST Control ID (Rev. 5)	NIST Control Name (Rev. 5)	ISO 27001/2:2013	FedRAMP	HITRUST	HIPAA Security Rule 45 C.F.R.	CIS Critical Security Controls v8	FERPA Privacy Technical Assistance Center (PTAC) Data Security Checklist	SOC2
PS-3	**Personnel Screening**	A.7.1.1	PS-3 (b)	02.b Screening	§§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), 164.312(e)	No Direct Mapping	Confirm the trustworthiness of employees through the use of personnel security screenings, policy training, and binding confidentiality agreements.	CC1.4
PS-4	**Personnel Termination**	A.7.3.1, A.8.1.4	PS-4 (a)	01.e Review of User Access Rights	§§164.308(a)(1)(ii)(C), 164.308(a)(3)	No Direct Mapping	No Direct Mapping	CC6.3
PS-5	**Personnel Transfer**	A.7.3.1, A.8.1.4	PS-5 (d)-2	01.e Review of User Access Rights	§§164.308(a)(1)(ii)(C), 164.308(a)(3)	No Direct Mapping	No Direct Mapping	CC6.3; CC5.4
PS-6	**Access Agreements**	A.7.1.2, A.7.2.1, A.13.2.4	PS-6 (b) PS-6 (c) (2)	02.c Terms and Conditions of Employment	§§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), 164.312(e)	No Direct Mapping	Conduct regular checks and trainings to ensure employee understanding of the terms and conditions of their employment	CC1.1
PS-7	**Third-Party Personnel Security**	A.6.1.1, A.7.2.1*	PS-7 (d)-2	02.d Management Responsibilities	§§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	No Direct Mapping	No Direct Mapping	CC9.2
PS-8	**Personnel Sanctions**	7.3, A.7.2.3	No Direct Mapping	02.f Disciplinary Process	§§164.308(a)(1)(ii)(C), 164.308(a)(3)	No Direct Mapping	No Direct Mapping	CC1.5
Risk Assessment (RA)								
RA-1	**Risk Assessment Policy and Procedures**	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2	RA-1 (b) (1) RA-1 (b) (2)	03.a Risk Management Program Development	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC3.2
RA-2	**Security Categorization**	A.8.2.1	No Direct Mapping	01.w Sensitive System Isolation	§§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)	CIS 3.7 - Establish and Maintain a Data Classification Scheme	No Direct Mapping	CC3.1

NIST Control ID (Rev. 5)	NIST Control Name (Rev. 5)	ISO 27001/2:2013	FedRAMP	HITRUST	HIPAA Security Rule 45 C.F.R.	CIS Critical Security Controls v8	FERPA Privacy Technical Assistance Center (PTAC) Data Security Checklist	SOC2
RA-3	**Risk Assessment**	6.1.2, 8.2, A.12.6.1*	RA-3 (b) RA-3 (c) RA-3 (d) RA-3 (e)	03.a Risk Management Program Development	§§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)	No Direct Mapping	No Direct Mapping	CC3.2
RA-4	**Risk Assessment Update**	**Withdrawn: Incorporated into RA-3**						No Direct Mapping
RA-5	**Vulnerability Scanning**	A.12.6.1*	RA-5 (a) RA-5 (d) RA-5 (e)	06.g Compliance with Security Policies and Standards	§§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)	CIS 7.1 - Establish and Maintain a Vulnerability Management Process CIS 7.2 - Establish and Maintain a Remediation Process CIS 7.5 - Perform Automated Vulnerability Scans of Internal Enterprise Assets	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.	CC7.1; CC4.1
RA-5 (2)	**Vulnerability Scanning – Frequency of Updates**	No Direct Mapping	No Direct Mapping	10.m Control of Technical Vulnerabilities	No Direct Mapping	CIS 7.7 - Remediate Detected Vulnerabilities	No Direct Mapping	CC7.1; CC4.2
RA-5 (5)	**Vulnerability Scanning – Privileged Access**	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC7.1; CC4.1
RA-6	**Technical Surveillance Countermeasures Survey**	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
RA-7	**Risk Response**	6.1.3, 8.3, 10.1	No Direct Mapping	No Direct Mapping	No Direct Mapping	CIS 7.7 - Remediate Detected Vulnerabilities	No Direct Mapping	No Direct Mapping
RA-9	**Criticality Analysis**	A.15.2.2*	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
System & Services Acquisition (SA)								
SA-1	**System and Services Acquisition Policy and Procedures**	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, 8.1, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2	SA-1 (b) (1) SA-1 (b) (2)	04.a Information Security Policy Document	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC5.2
SA-2	**Allocation of Resources**	No Direct Mapping	No Direct Mapping	05.b Information Security Coordination	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC8.1
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	No Direct Mapping	05.c Allocation of Information Security Responsibilities	§§164.308(a)(1)(i)	No Direct Mapping	No Direct Mapping	CC8.1
SA-4	**Acquisition Process**	8.1, A.14.1.1, A.14.2.7, A.14.2.9, A.15.1.2	SA-4	09.i System Acceptance	§§164.308(a)(1)(i), 164.308(a)(1)(ii)(D)	CIS 15.4 - Assess Service Providers	No Direct Mapping	CC8.1
SA-4 (1)	**Acquisition Process – Functional Properties of Controls**	No Direct Mapping	No Direct Mapping	10.a Security Requirements Analysis and Specification	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC8.1
SA-4 (2)	**Acquisition Process – Design and Implementation Information for Controls**	No Direct Mapping	No Direct Mapping	10.a Security Requirements Analysis and Specification	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC8.1
SA-4 (9)	**Acquisition Process – Functions, Ports, Protocols, and Services in Use**	No Direct Mapping	No Direct Mapping	10.a Security Requirements Analysis and Specification	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC8.1
SA-4 (10)	**Acquisition Process – Use of Approved PIV Products**	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC8.1

NIST Control ID (Rev. 5)	NIST Control Name (Rev. 5)	ISO 27001/2:2013	FedRAMP	HITRUST	HIPAA Security Rule 45 C.F.R.	CIS Critical Security Controls v8	FERPA Privacy Technical Assistance Center (PTAC) Data Security Checklist	SOC2
SA-5	Information System Documentation	7.5.1, 7.5.2, 7.5.3, A.12.1.1*	No Direct Mapping	09.r Security of System Documentation	§§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)	No Direct Mapping	No Direct Mapping	CC8.1
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.14.2.5	No Direct Mapping	10.a Security Requirements Analysis and Specification	§§164.308(a)(1)(i)	CIS 12.2 - Establish and Maintain a Secure Network Architecture	No Direct Mapping	CC8.1
SA-9	External Information System Services	A.6.1.1, A.6.1.5, A.7.2.1, A.13.1.2, A.13.2.2, A.15.2.1, A.15.2.2	SA-9 (a) SA-9 (c)	05.k Addressing Security in Third Party Agreements	§§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)	CIS 15.2 - Establish and Maintain a Service Provider Management Policy	No Direct Mapping	CC9.2
SA-9 (2)	External System Services – Identification of Functions/Ports/Protocols/Services	No Direct Mapping	No Direct Mapping	09.n Security of Network Services	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC9.2
SA-10	Developer Configuration Management	A.12.1.2, A.14.2.2, A.14.2.4, A.14.2.7	No Direct Mapping	09.d Separation of Development, Test, and Operational Environments	§§164.308(a)(1)(i), 164.308(a)(8), 164.308(a)(7)(i), 164.308(a)(7)(ii)	No Direct Mapping	No Direct Mapping	CC8.1
SA-11	Developer Security Testing and Evaluation	A.14.2.7, A.14.2.8	No Direct Mapping	09.i System Acceptance	§§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)	No Direct Mapping	No Direct Mapping	CC8.1
SA-12	Supply Chain Protections	Withdrawn: Incorporated into SR Family						
SA-13	Trustworthiness	Withdrawn: Incorporated into SA-8						
SA-14	Criticality Analysis	Withdrawn: Incorporated into RA-9						
SA-15	Development Process, Standards, and Tools	A.6.1.5, A.14.2.1	No Direct Mapping	10.a Security Requirements Analysis and Specification	§§164.308(a)(1)(i)	No Direct Mapping	No Direct Mapping	No Direct Mapping
SA-15 (3)	Development Process, Standards, and Tools – Criticality Analysis	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
SA-16	Developer-Provided Training	No Direct Mapping	No Direct Mapping	02.e Information Security Awareness, Education, and Training	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
SA-17	Developer Security Architecture and Design	A.14.2.1, A.14.2.5	No Direct Mapping	10.a Security Requirements Analysis and Specification	§§164.308(a)(1)(i)	No Direct Mapping	No Direct Mapping	No Direct Mapping
SA-18	Tamper Resistance and Detection	Withdrawn: Incorporated into SR-9						
SA-19	Component Authenticity	Withdrawn: Incorporated into SR-11						
SA-20	Customized Development of Critical Components	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
SA-21	Developer Screening	A.7.1.1	No Direct Mapping	No Direct Mapping	No Direct Mapping		No Direct Mapping	No Direct Mapping
SA-22	Unsupported System Components	No Direct Mapping	No Direct Mapping	10.h Control of Operational Software	No Direct Mapping	CIS 2.2 - Ensure Authorized Software is Currently Supported	No Direct Mapping	No Direct Mapping
System & Communications Protection (SC)								
SC-1	System and Communications Protection Policy and Procedures	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, 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)	04.a Information Security Policy Document	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC5.2
SC-2	Application Partitioning	No Direct Mapping	No Direct Mapping	01.s Use of System Utilities	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC6.1
SC-3	Security Function Isolation	No Direct Mapping	No Direct Mapping	09.k Controls Against Mobile Code	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
SC-4	Information In Shared Resources	No Direct Mapping	No Direct Mapping	01.w Sensitive System Isolation	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC6.1

NIST Control ID (Rev. 5)	NIST Control Name (Rev. 5)	ISO 27001/2:2013	FedRAMP	HITRUST	HIPAA Security Rule 45 C.F.R.	CIS Critical Security Controls v8	FERPA Privacy Technical Assistance Center (PTAC) Data Security Checklist	SOC2
SC-5	**Denial of Service Protection**	No Direct Mapping	No Direct Mapping	09.h Capacity Management	§§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)	No Direct Mapping	No Direct Mapping	CC6.1; A1.1
SC-6	**Resource Availability**	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
SC-7	**Boundary Protection**	A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.3	No Direct Mapping	01.m Segregation in Networks	§§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)	CIS 4.5 - Implement and Manage a Firewall on End-User Devices CIS 13.4 - Perform Traffic Filtering Between Network Segments CIS 13.5 - Manage Access Control for Remote Assets	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.	CC6.6
SC-7 (3)	**Boundary Protection - Access Points**	No Direct Mapping	No Direct Mapping	01.n Network Connection Control	No Direct Mapping	CIS 9.3 - Maintain and Enforce Network-Based URL Filters	No Direct Mapping	CC6.6
SC-7 (4)	**Boundary Protection – External Telecommunications Services**	No Direct Mapping	No Direct Mapping	01.n Network Connection Control	No Direct Mapping	CIS 9.3 - Maintain and Enforce Network-Based URL Filters	No Direct Mapping	CC6.6
SC-7 (5)	**Boundary Protection – Deny By Default – Allow By exception**	No Direct Mapping	No Direct Mapping	01.n Network Connection Control	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC6.6
SC-7 (7)	**Boundary Protection – Split Tunneling For Remote Devices**	No Direct Mapping	No Direct Mapping	01.n Network Connection Control	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC6.6
SC-7 (8)	**Boundary Protection- Route Traffic to Authenticated Proxy Servers**	No Direct Mapping	No Direct Mapping	01.n Network Connection Control	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
SC-8	**Transmission Confidentiality and Integrity**	A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3	No Direct Mapping	01.n Network Connection Control	§§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), 164.314(b)(2)(i)	No Direct Mapping	No Direct Mapping	CC6.7
SC-8 (1)	**Transmission Confidentiality and Integrity – Cryptographic Protection**	No Direct Mapping	No Direct Mapping	05.i Identification of Risks Related to External Parties	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC6.7
SC-9	**Transmission Confidentiality**	**Withdrawn: Incorporated into SC-8**						
SC-10	**Network Disconnect**	A.13.1.1	No Direct Mapping	01.g Unattended User Equipment	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC6.6
SC-11	**Trusted Path**	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
SC-12	**Cryptographic Key Establishment and Management**	A.10.1.2	SC-12	10.g Key Management	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC6.1

NIST Control ID (Rev. 5)	NIST Control Name (Rev. 5)	ISO 27001/2:2013	FedRAMP	HITRUST	HIPAA Security Rule 45 C.F.R.	CIS Critical Security Controls v8	FERPA Privacy Technical Assistance Center (PTAC) Data Security Checklist	SOC2
SC-13	Cryptographic Protection	A.10.1.1, A.14.1.2, A.14.1.3, A.18.1.5	SC-13	06.f Regulation of Cryptographic Controls	§§164.308(a)(1)(ii)(D), 164.308(a)(3), 164.308(a)(4), 164.310(b), 164.310(c), 164.312(a), 164.312(e)	No Direct Mapping	No Direct Mapping	CC6.1
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						No Direct Mapping
SC-15	Collaborative Computing Devices	A.13.2.1*	SC-15 (a)	01.v Information Access Restriction	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC6.1
SC-16	Transmission of Security Attributes	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
SC-17	Public Key Infrastructure Certificates	A.10.1.2	No Direct Mapping	10.g Key Management	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC6.1
SC-18	Mobile Code	No Direct Mapping	No Direct Mapping	09.k Controls Against Mobile Code	§§164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B)	No Direct Mapping	No Direct Mapping	CC6.8
SC-19	Voice Over Internet Protocol	Withdrawn: Moved to SR-11						CC6.1
SC-20	Secure Name/Address Resolution Service (Authoritative Source)	No Direct Mapping	No Direct Mapping	09.m Network Controls	No Direct Mapping	CIS 4.9 - Configure Trusted DNS Servers on Enterprise Assets	No Direct Mapping	CC6.1
SC-21	Secure Name/Address Resolution Service (Recursive or Caching Resolver)	No Direct Mapping	No Direct Mapping	09.m Network Controls	No Direct Mapping	CIS 4.9 - Configure Trusted DNS Servers on Enterprise Assets	No Direct Mapping	CC6.1
SC-22	Architecture and Provisioning for Name/Address Resolution Service	No Direct Mapping	No Direct Mapping	09.m Network Controls	No Direct Mapping	CIS 4.9 - Configure Trusted DNS Servers on Enterprise Assets	No Direct Mapping	A1.1
SC-23	Session Authenticity	No Direct Mapping	No Direct Mapping	09.m Network Controls	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC6.1
SC-24	Fail in Known State	No Direct Mapping	No Direct Mapping	08.a Physical Security Perimeter	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
SC-25	Thin Nodes	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
SC-26	Honeypots	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
SC-27	Platform-Independent Applications	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
SC-28	Protection of Information at Rest	A.8.2.3*	No Direct Mapping	06.d Data Protection and Privacy of Covered Information	§§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)	No Direct Mapping	No Direct Mapping	CC6.1
SC-29	Heterogeneity	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC6.1
SC-30	Concealment and Misdirection	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
SC-31	Covert Channel Analysis	No Direct Mapping	No Direct Mapping	No Direct Mapping	§§164.308(a)(1)(ii)(D), 164.308(a)(3), 164.308(a)(4), 164.310(b), 164.310(c), 164.312(a), 164.312(e)	No Direct Mapping	No Direct Mapping	No Direct Mapping
SC-32	Information System Partitioning	No Direct Mapping	No Direct Mapping	01.m Segregation in Networks	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
SC-33	Transmission Preparation Integrity	Withdrawn: Incorporated into SC-8						No Direct Mapping
SC-34	Non-Modifiable Executable Programs	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
SC-35	Honeyclients	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
SC-36	Distributed Processing and Storage	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
SC-37	Out-of-Band Channels	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
SC38	Operations Security	A.12.x	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
SC-39	Process Isolation	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping

NIST Control ID (Rev. 5)	NIST Control Name (Rev. 5)	ISO 27001/2:2013	FedRAMP	HITRUST	HIPAA Security Rule 45 C.F.R.	CIS Critical Security Controls v8	FERPA Privacy Technical Assistance Center (PTAC) Data Security Checklist	SOC2
SC-40	**Wireless Link Protection**	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
SC-41	**Port and I/O Device Access**	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
SC-42	**Sensor Capability and Data**	A.11.1.5*	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
SC-43	**Usage Restrictions**	No Direct Mapping	No Direct Mapping	01.u Limitation of Connection Time	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
SC-44	**Detonation Chambers**	No Direct Mapping	No Direct Mapping	No Direct Mapping	§§164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B)	No Direct Mapping	No Direct Mapping	No Direct Mapping
				System & Information Integrity (SI)				
SI-1	**System and Information Integrity Policy and Procedures**	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, 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)	04.a Information Security Policy Document	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC5.2
SI-2	**Flaw Remediation**	A.12.6.1, A.14.2.2, A.14.2.3, A.16.1.3	SI-2 (c)	10.c Control of Internal Processing	§§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)	CIS 7.3 - Perform Automated Operating System Patch Management CIS 7.4 - Perform Automated Application Patch Management CIS 7.7 - Remediate Detected Vulnerabilities	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.	CC8.1
SI-2 (2)	**Flaw Remediation – Automated Flaw Remediation Status**	No Direct Mapping	No Direct Mapping	10.m Control of Technical Vulnerabilities	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC8.1
SI-3	**Malicious Code Protection**	A.12.2.1	SI-3 (c) (1)-1 SI-3 (c) (1)-2 SI-3 (c) (2)	09.ab Monitoring System Use	§§164.306(e), 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B)	CIS 10.1 - Deploy and Maintain Anti-Malware Software CIS 10.2 - Configure Automatic Anti-Malware Signature Updates CIS 10.4 - Configure Automatic Anti-Malware Scanning of Removable Media	No Direct Mapping	CC6.8
SI-4	**Information System Monitoring**	No Direct Mapping	SI-4	01.x Mobile Computing and Communications	§§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), 164.316(b)(2)(iii)	CSI 1.3 - Utilize an Active Discovery Tool CIS 1.5 - Use a Passive Asset Discovery Tool CIS 7.6 - Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets CIS 13.3 - Deploy a Network Intrusion Detection Solution CIS 13.5 - Manage Access Control for Remote Assets CIS 13.6 - Collect Network Traffic Flow Logs CIS 13.8 - Deploy a Network Intrusion Prevention Solution CIS 13.11 - Tune security event alerting thresholds monthly, or more frequently.	Shut down unnecessary services as each port, protocol, or service is a potential avenue for ingress into the network.	CC7.2
SI-4 (2)	**System Monitoring – Automated Tools for Real-Time Analyses**	No Direct Mapping	No Direct Mapping	09.ab Monitoring System Use	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC7.2
SI-4 (4)	**System Monitoring – Inbound and Outbound Communications Traffic**	No Direct Mapping	No Direct Mapping	09.ab Monitoring System Use	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC7.2
SI-4 (5)	**System Monitoring – System Generated Alerts (Moderate**	No Direct Mapping	No Direct Mapping	09.ab Monitoring System Use	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC7.2

NIST Control ID (Rev. 5)	NIST Control Name (Rev. 5)	ISO 27001/2:2013	FedRAMP	HITRUST	HIPAA Security Rule 45 C.F.R.	CIS Critical Security Controls v8	FERPA Privacy Technical Assistance Center (PTAC) Data Security Checklist	SOC2
SI-5	**Security Alerts, Advisories, and Directives**	A.6.1.4*	SI-5 (a) SI-5 (c)	05.g Contact with Special Interest Groups	§§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)	CIS 8.2 - Collect Audit Logs CIS 17.3 - Establish and Maintain an Enterprise Process for Reporting Incidents	No Direct Mapping	CC7.3
SI-6	**Security Function Verification**	No Direct Mapping	No Direct Mapping	10.c Control of Internal Processing	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
SI-7	**Software, Firmware, and Information Integrity**	No Direct Mapping	No Direct Mapping	10.c Control of Internal Processing	§§164.308(a)(1)(ii)(D), 164.312(b), 164.312(c)(1), 164.312(c)(2), 164.312(e)(2)(i)	No Direct Mapping	No Direct Mapping	CC7.2
SI-7 (1)	**Software, Firmware, and Information Integrity – Integrity Checks**	No Direct Mapping	No Direct Mapping	10.c Control of Internal Processing	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC7.2
SI-7 (7)	**Software, Firmware, and Information Integrity – Integration of Detection and Response**	No Direct Mapping	No Direct Mapping	10.c Control of Internal Processing	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC7.2
SI-8	**Spam Protection**	No Direct Mapping	No Direct Mapping	09.j Controls Against Malicious Code	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC6.8
SI-8 (1)	**Spam Protection – Central Management**	No Direct Mapping	No Direct Mapping	09.j Controls Against Malicious Code	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC6.8
SI-8 (2)	**Spam Protection – Automatic Updates**	No Direct Mapping	No Direct Mapping	09.j Controls Against Malicious Code	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC6.8
SI-9	**Information Input Restrictions**	**Withdrawn: Incorporated into AC-2, AC-3, AC-5, AC-6**						No Direct Mapping
SI-10	**Information Input Validation**	No Direct Mapping	No Direct Mapping	10.b Input Data Validation	No Direct Mapping	No Direct Mapping	No Direct Mapping	PI1.2
SI-11	**Error Handling**	No Direct Mapping	No Direct Mapping	09.ae Fault Logging	No Direct Mapping	No Direct Mapping	No Direct Mapping	PI1.3
SI-12	**Information Handling and Retention**	No Direct Mapping	No Direct Mapping	06.c Protection of Organizational Records	No Direct Mapping	No Direct Mapping	No Direct Mapping	PI1.3
SI-13	**Predictable Failure Prevention**	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
SI-14	**Non-Persistence**	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
SI-15	**Information Output Filtering**	No Direct Mapping	No Direct Mapping	10.e Output Data Validation	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
SI-16	**Memory Protection**	No Direct Mapping	No Direct Mapping	09.j Controls Against Malicious Code	No Direct Mapping	No Direct Mapping	No Direct Mapping	CC6.1
SI-17	**Fail-Safe Procedures**	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
				Supply Chain Risk Management				
SR-1	**Supply Chain Risk Management Policy and Procedures**	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.15.1.1, A.18.1.1, A.18.2.2	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
SR-2	**Supply Chain Risk Management Plan**	A.14.2.7*	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
SR-2 (1)	**Supply Chain Risk Management Plan - Establish SCRM Team**	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
SR-3	**Supply Chain Controls and Processes**	A.15.1.2, A.15.1.3*	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
SR-5	**Acquisition Strategies, Tools and Methods**	A.15.1.3	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
SR-6	**Supplier Assessments and Reviews**	A.15.2.1	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
SR-8	**Notification Agreements**	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
SR-10	**Inspection of Systems or Components**	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
SR-11	**Component Authenticity**	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
SR-11 (1)	**Component Authenticity - Anti – Counterfeit Training**	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping

NIST Control ID (Rev. 5)	NIST Control Name (Rev. 5)	ISO 27001/2:2013	FedRAMP	HITRUST	HIPAA Security Rule 45 C.F.R.	CIS Critical Security Controls v8	FERPA Privacy Technical Assistance Center (PTAC) Data Security Checklist	SOC2
SR-11 (2)	**Component Authenticity | Configuration Control for Component Service and Repair**	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping
SR-12	**Component Disposal**	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping	No Direct Mapping