Wingify

Wingify- NIST 800-53 Rev.4 Crosswalk with HIPAA and ISO 27001/2:2013 Assessment

HIPAA Safeguard	NIST SP800-53 R4: Control #	Control Question #	NIST Control Name	HIPAA CFR Control Reference(s)	ISO 27001/2 : 2013	Control Assessment Questions:	Wingify Control Assessment Answers
Access Control	AC-1	AC-1.1	ACCESS CONTROL POLICY AND PROCEDURES	164.308(a)(3)(i), 164.308(a)(3)(ii)(A), 164.308(a)(4)(i), 164.308(a)(4)(ii)(B), 164.308(a)(4)(ii)(C, 164.312(a)(1)	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	Are there formally documented policies and procedures for access control?	**Yes**
	AC-2	AC-2.1	ACCOUNT MANAGEMENT	164.308(a)(3)(ii)(B), 164.308(a)(4)(i), 164.308(a)(4)(ii)(B), 164.308(a)(4)(ii)(C, 164.308(a)(5)(ii)(C, 164.312(a)(2)(i), 164.312(a)(2)(ii)	A.6.1.2, A.9.1.2, A.9.2.1, 9.2.2, A.9.2.3, A.9.2.4, A.9.2.5, A.9.2.6, A.9.3.1, A.9.4.1, A.9.4.2, A.9.4.3, A.9.4.4, A.12.4.1, A.18.2.2	Do you have a process for managing accounts, including - creating, modifying, monitoring, and deleting/disabling accounts?	**Yes**
		AC-2.2				Are accounts reviewed on a periodic basis as per control requirement?	**Yes**
		AC-2.3				Have all guest, shared (other than Admin/Root), or group accounts been removed or disabled?	**Yes**
		AC-2.4				Are account managers notified when accounts are no longer required, when users are terminated or transferred, or when individual access requirements change?	**Partial**
		AC-2.5				Is approval from an authorized signer required before provisioning accounts?	**Yes**
	AC-3	AC-3.1	ACCESS ENFORCEMENT	164.308(a)(3)(ii)(A), 164.308(a)(4)(ii)(B), 164.308(a)(4)(ii)(C, 164.310(a)(2)(iii), 164.310(b), 164.312(a)(1), 164.312(a)(2)(i), 164.312(a)(2)(ii), 164.312(a)(2)(iv)	A.6.2.2, A.9.1.2, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.1, A.13.2.1, A.14.1.2, A.14.1.3, A.18.1.3	Does the information system verify the rights of a user to access the information system? (Access Control Lists, Group/Role membership?)	**Yes**
		AC-3.2				Does the information system support role-based account management and access controls (RBAC)?	**Yes**
		AC-3.3				If RBAC is supported, can a customer administrator create/customize unique roles and permissions.	**Partial**
	AC-4	AC-4.1	INFORMATION FLOW ENFORCEMENT	164.308(a)(3)(ii)(A), 164.308(a)(4)(ii)(B), 164.310(b)	A.6.2.2, A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3	Is the flow of sensitive information secured between interconnected systems? (Firewall rule sets - iptables, proxies, encrypted tunnels.)	**Yes**
	AC-5	AC-5.1	SEPARATION OF DUTIES	164.308(a)(3)(i), 164.308(a)(4)(i), 164.308(a)(4)(ii)(A), 164.312(a)(1)	A.6.1.1, A.6.1.2, A.9.1.1, A.9.1.2, A.12.1.3	Is separation of duties implemented? (E.g., Mission functions and support functions divided among personnel, different administrative accounts for different roles.)	**Yes**
	AC-6	AC-6.1	LEAST PRIVILEGE	164.308(a)(3)(i), 164.308(a)(4)(i), 164.308(a)(4)(ii)(A), 164.312(a)(1)	A.6.1.1, A.9.1.1, A.9.1.2, A.9.2.1, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5	Is least privilege employed? (I.e., must administrators switch to the root or a separate administrator account to perform administrative functions/make system changes?)	**Yes**
	AC-11	AC-11.1	SESSION LOCK	164.310(b), 164.312(a)(2)(iii)	A.9.4.2, A.11.2.8, A.11.2.9	Does the application/system have a session lock after a period of inactivity that requires a user to reauthenticate?	**Yes**
	AC-12	AC-12.1	SESSION TERMINATION	164.310(b), 164.312(a)(2)(iii)		Does the application/system terminate the session after predefined circumstances?	**Yes**
	AC-13	AC-13.1	SUPERVISION AND REVIEW ACCESS CONTROL	164.308(a)(3)(ii)(A), 164.308(a)(4)(i), 164.308(a)(4)(ii)(B), 164.308(a)(5)(ii)(C		Does the access control review process in place?	**Yes**
	AC-17	AC-17.1	REMOTE ACCESS	164.310(b)	A.6.2.1, A.6.2.2, A.9.1.1, A.9.1.2, A.13.1.1, A.13.2.1, A.14.1.2	Is remote access allowed from outside the network only through the use of the VPN client?	**Yes**
		AC-17.2				Are there established and documented usage restrictions for those connections?	**Yes**
		AC-17.3				Is remote access to the information system authorized prior to allowing such connections?	**Yes**
	AC-18	AC-18.1	WIRELESS ACCESS	164.308(a)(1)(ii)(D) 164.312(a)(1), 164.312(b), 164.312(E)	A.6.2.1, A.6.2.2, A.9.1.1, A.9.1.2, A.10.1.1, A.13.1.1, A.13.2.1	Does the information system and/or associated device allow wireless access and only connect to secure networks? (Network access, Bluetooth, infrared, etc.)	**Yes**
	AC-19	AC-19.1	ACCESS CONTROL FOR MOBILE DEVICES	164.310(b)	A.6.2.1, A.9.1.1, A.11.2.6, A.12.2.1, A.13.2.1	Can users or administrators connect using mobile devices (i.e. iPad, Smart Phone, PDAs)?	**Partial**
		AC-19.2				Are there established and documented usage restrictions for those connections?	**Yes**
		AC-19.3				Is remote access to the information system authorized prior to allowing such connections?	**Yes**
	AT-1	AT-1.1	SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES	164.308(a)(5)(i)	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A18.2.2	Are there formally documented procedures for security awareness and training for this information system?	**Yes**

Awareness and Trainin	AT-2	AT-2.1	SECURITY AWARENESS	164.308(a)(5)(i), 164.308(a)(5)(ii)(A), 164.308(a)(5)(ii)(B)	A.6.1.1, A.7.2.2, A.11.1.5, A.12.2.1	Is basic security awareness training performed for all personnel as a part of the onboarding process?	**Yes**
		AT-2.2				Is it periodically performed for all users?	**Yes**
	AT-3	AT-3.1	SECURITY TRAINING	164.308(a)(5)(i)	Clause 7.2(a), 7.2(b) A.6.1.1, A.7.2.2, A.11.1.5 , A.9.3.1 A.11.2.8	Is there role-based security training for personnel with assigned security roles and responsibilities for this information system before access is granted and when required by information system changes?	**Yes**
	AT-4	AT-4.1	SECURITY TRAINING RECORDS	164.308(a)(5)(i)	Clause 7.2(a), 7.2(b) A.7.2.2,A.9.3.1 A.11.2.8	Do you document and monitor information system security training activities for individuals?	**Yes**
Audit and Accountability	AU-1	AU-1.1	AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES	164.312(b)	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.12.1.2, A.12.4.1, A.12.7.1, A.18.1.1, A.18.2.2	Are there formally documented audit and accountability procedures for this information system?	**Yes**
	AU-2	AU-2.1	AUDITABLE EVENTS	164.308(a)(5)(ii)(C, 164.312(b)	A.12.1.1, A.12.4.1, A.12.4.3, A.12.7.1	Is the information system actively auditing events such as access to patient information, login/logoffs, account creation, etc.?	**N/A**
		AU-2.2				Are the audit logs captured sufficient for incident response and system and user performance/investigation?	**Yes**
	AU-3	AU-3.1	CONTENT OF AUDIT RECORDS	164.312(b)	A.12.1.1, A.12.4.1	Does the system create audit records that contain sufficient information to, at a minimum, establish what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event?	**Yes**
	AU-4	AU-4.1	AUDIT STORAGE CAPACITY	164.312(b)	A.12.1.1, A.12.1.3, A.12.4.1	Have you evaluated the audit storage capacity of this information system and determined that it is adequate?	**Yes**
	AU-6	AU-6.1	AUDIT REVIEW, ANALYSIS, AND REPORTING	164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(C, 164.312(b)	A.12.1.2, A.12.4.1, A.16.1.2, A.16.1.4	Do you review the audit logs for indications of inappropriate or unusual activity and report those incidents to authorized personnel?	**Yes**
	AU-8	AU-8.1	TIME STAMPS	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)	A.12.1.1, A.12.4.1, A.12.12.4	Are the audit logs time stamped? (Date and Time)	**Yes**
	AU-9	AU-9.1	PROTECTION OF AUDIT INFORMATION	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)	A.12.4.2, A.12.4.3, A.16.1.7, A.18.1.3	Does the system/application protect audit information from unauthorized access, modification, and deletion?	**Yes**
	AU-11	AU-11.1	AUDIT RECORD RETENTION	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	A.12.1.1, A.12.4.1, A.16.1.7, A.18.1.3	Does the information system retain audit records in accordance with implemented policies?	**Yes**
Security Assessment and Authorization	CA-1	CA-1.1	SECURITY ASSESSMENT AND AUTHORIZATION POLICIES AND PROCEDURES	164.308(a)(8)	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2	Are there formally documented policies and procedures for Security Assessments and Authorizations?	**Yes**
	CA-2	CA-2.1	SECURITY ASSESSMENTS	164.308(a)(8)	A.14.2.8, A.14.2.9, A.15.1.1, A.15.1.2, A.18.2.1, A.18.2.2, A.18.2.3	Has the scope of the security assessment plan been addressed, and does it cover specific security controls and enhancements?	**Yes**
		CA-2.2				Are interconnection security agreements documented? (e.g. interface characteristics, security requirements, data types transmitted)	**Yes**
		CA-2.3				Are these connections monitored for compliance with the agreements?	**Yes**
	CA-3	CA-3.1	INFORMATION SYSTEM CONNECTIONS	164.308(b)(1), 164.308(b)(4), 164.314(a)(2)(ii)	A.13.1.1, A.13.1.2, A.13.2.1, A.13.2.2, A.15.1.1, A.15.1.2	Does this information system interface with any other information system?	**No**
		CA-3.2				Are the interfaces that interconnect with this information system documented?	**No**
		CA-3.3				Is there documentation on what information is communicated through that interface and what the security requirements are?	**No**
	CA-6	CA-6.1	SECURITY AUTHORIZATION		A.14.2.9	Is there an authorizing official for environment? Can they decide if an environment is turned off if necessary?	**Yes**
	CA-7	CA-7.1	CONTINUOUS MONITORING	164.308(b)(1), 164.308(b)(4), 164.314(a)(2)(ii)	A.18.2.1, A.18.2.2, A.18.2.3	Is there a continuous monitoring strategy? What metrics are used to ensure compliance?	**Yes**
		CA-7.2				Are continuous monitoring results analyzed?	**Yes**
		CA-7.3				Are security controls monitored for compliance?	**Yes**
		CA-7.4				Are the results of continuous monitoring reported to an authorizing official?	**Yes**

Contingency Planning	CP-1		CONTINGENCY PLANNING POLICY AND PROCEDURES	164.308(a)(7)(i)	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.17.1.1, A.18.1.1, A.18.2.2	Are there formally documented policies and procedures for Contingency Plan?	**Yes**
	CP-2	CP-2.1	CONTINGENCY PLAN	164.308(a)(7)(ii)(B), 164.308(a)(7)(ii)(C, 164.308(a)(7)(ii)(E, 164.310(a)(2)(i), 164.312(a)(2)(ii)	A.6.1.1, A.11.1.4, A.17.1.1, A.17.1.3, A.17.2.1	Have you developed a contingency plan for this information system?	**Yes**
		CP-2.2				Does the contingency plan: - Identify the essential missions and business functions - Provide recovery objectives, restoration priorities, and metrics - Address contingency roles, responsibilities, and assigned individuals with contact information - Address maintaining essential missions and business functions despite a disruption - Address full restoration without deterioration of originally implemented security safeguards - Distributed to key personnel - Coordinated with incident handling procedures - Reviewed and updated to address changes - Protected from unauthorized disclosure or modification	**Yes**
	CP-3	CP-3.1	CONTINGENCY TRAINING	164.308(a)(7)(ii)(D)	A.7.2.2, A.11.1.4	Does your department train personnel in their contingency roles and responsibilities and provide refresher training when required?	**Yes**
	CP-4	CP-4.1	CONTINGENCY PLAN TESTING AND EXERCISES	164.308(a)(7)(ii)(D)	A.11.1.4, A.17.1.1, A.17.1.3	Do you test and/or exercise the contingency plan periodically to determine the plan's effectiveness and review the contingency plan test results to initiate any needed corrective actions?	**Yes**
	CP-5		CONTINGENCY PLAN UPDATE	164.308(a)(7)(ii)(D)			
	CP-6	CP-6.1	ALTERNATE STORAGE SITE	164.308(a)(7)(ii)(B), 164.310(a)(2)(i)	A.11.1.4, A.17.1.2, A.17.2.1	Has your department established an alternate storage site including necessary agreements to permit the storage and recovery of information system backup information?	**Yes**
		CP-6.2				Does the alternate storage site provide information security safeguards equivalent to that of the primary site?	**Partial**
	CP-7	CP-7.1	ALTERNATE PROCESSING SITE	164.308(a)(7)(ii)(B), 164.310(a)(2)(i)	A.11.1.4, A.17.1.2, A.17.2.1	Has your department established an alternate processing site to permit the resumption of information system operations for essential missions and business functions when the primary processing capabilities are unavailable?	**Partial**
		CP-7.2				Does the alternate processing site provide information security safeguards equivalent to that of the primary site?	**Partial**
	CP-9	CP-9.1	INFORMATION SYSTEM BACKUP	164.308(a)(7)(ii)(A), 164.308(a)(7)(ii)(B), 164.310(d)(2)(iv), 164.312(c)(1)	A.11.1.4, A.12.3.1, A.17.1.2, A.18.1.3	Is user-level information, system-level information, and information system documentation backed up?	**Yes**
		CP-9.2				Is the confidentiality, integrity, and availability of backup information protected at the storage location?	**Yes**
Authentication	IA-1	IA-1.1	IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURE	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)	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2	Does the application/system use managed LDAP services for identification and authentication?	**Partial**
		IA-1.2				Are there formally documented policies and procedures for Identification and Authentication?	**Yes**
	IA-2	IA-2.1	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)	164.308(a)(5)(ii)(D), 164.312(a)(2)(i), 164.312(d)	A.9.2.1, A.9.3.1, A.9.4.2, A.9.4.3, A.11.2.8	Does the information system use multifactor authentication for privileged or non-privileged access? (Uses at least two of: what you have, what you know, what you are. E.g., tokens, passwords, biometrics.)	**Partial**
	IA-3	IA-3.1	DEVICE IDENTIFICATION AND AUTHENTICATION	164.312(a)(2)(i), 164.312(d)		Does the information system uniquely identify and authenticate devices before establishing a connection? (E.g., MAC, TCP/IP, IEEE 802.1x)	**Yes**
	IA-4	IA-4.1	IDENTIFIER MANAGEMENT	164.308(a)(5)(ii)(D), 164.312(a)(2)(i), 164.312(d)	A.9.2.1, A.16.1.6, A.16.1.7	Do you manage the information system identifiers for users and devices by requiring authorization by an authorized signer prior to assigning an identifier?	**Yes**
		IA-4.2				Does the application/system prevent reuse of user or device identifiers?	**Yes**
		IA-4.3				Does the application/system disable the user or device account after a pre-defined period of inactivity?	**Yes**
	IA-5	IA-5.1	AUTHENTICATOR MANAGEMENT	164.308(a)(5)(ii)(D)	A.9.2.1, A.9.2.3, A.9.2.4, A.9.3.1, A.9.4.3	Does the application/system comply with the password complexity as outlined in implemented policies?	**Yes**

Identification and		IA-5.2				Does the End User comply with password requirements regarding complexity, length and change? - Are Passwords at least 8 characters in length? - Are Passwords created using the following:? - Mixed case alpha characters - at least one numeric digit	**Partial**
		IA-5.3				Are the passwords encrypted within the information system when stored or transmitted?	**Yes**
		IA-5.4				Are factory default passwords changed once implemented into production? (Admin/root passwords.)	**Yes**
		IA-5.5				Are there administrative procedures for initial password distribution and for revoking access?	**Yes**
		IA-5.6				Is authenticator content protected from unauthorized disclosure and modification?	**Yes**
		IA-5.7				Are passwords for group/role accounts changed when membership to those accounts change?	**Yes**
	IA-6	IA-6.1	AUTHENTICATOR FEEDBACK	164.308(a)(5)(ii)(D)	A.9.4.2	Does the information system obscure the authenticator/password during the authentication process?	**Yes**
	IA-7	IA-7.1	CRYPTOGRAPHIC MODULE AUTHENTICATION	164.308(a)(5)(ii)(D)	A.10.1.1, A.18.1.1, A.18.1.5, A.18.2.2	Does the information system use mechanisms for authentication to a cryptographic module? (This control is used for mostly operating systems and appliances used to encrypt something.)	**Yes**
Incident Response	IR-1	IA-1.1	INCIDENT RESPONSE POLICY AND PROCEDURES	164.308(a)(6)(i)	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.16.1.1, A.16.1.2, A.18.1.1, A.18.2.2	Are there formally documented policies and procedures for Incident Response?	**Yes**
	IR-2	IR-2.1	INCIDENT RESPONSE TRAINING	164.308(a)(6)(i)	A.7.2.2	Are staff provided with incident response training?	**Yes**
		IR-2.2				Is incident response training unique based on the role of the individual?	**Yes**
	IR-3	IR-3.1	INCIDENT RESPONSE TESTING AND EXERCISES	164.308(a)(2), 164.308(a)(7)(ii)(A), 164.308(a)(7)(ii)(B), 164.308(a)(7)(ii)(C), 164.308(a)(7)(ii)(D), 164.310(a)(2)(i),		Are incident response tests conducted?	**Yes**
		IR-3.2				Are the incident response test results analyzed?	**Yes**
	IR-4	IR-4.1	INCIDENT HANDLING	§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),	A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7	Is there an incident handling process	**Yes**
		IR-4.2				Are incident handling activities coordinated with contingency planning activities?	**Yes**
	IR-5	IR-5.1	INCIDENT MONITORING	164.308(a)(1)(ii)(D), 164.308(a)(6)(ii)		Are security incidents tracked and documented?	**Yes**
	IR-6	IR-6.1	INCIDENT REPORTING	164.308(a)(1)(ii)(D), 164.308(a)(6)(ii), 164.314(a)(2)(i)	A.6.1.3, A.16.1.2	Are security incidents timely reported to appropriate personnel/ government authorities?	**Yes**
	IR-7	IR-7.1	INCIDENT RESPONSE ASSISTANCE	164.308(a)(6)(ii)		Are incident response resources used outside of the incident response team?	**Partial**
Maintenance	MA-1		SYSTEM MAINTENANCE POLICY AND PROCEDURES	164.310(a)(2)(iv)	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2	Are there formally documented policies and procedures for Maintenance?	**Partial**
	MA-2	MA-2.1	CONTROLLED MAINTENANCE	164.308(a)(3)(ii)(A) 164.310(a)(2)(iv)	A.11.2.4, A.11.2.5	Are maintenance and repairs on the information system scheduled, performed, documented, and reviewed?	**Partial**
		MA-2.2				Do you approve and monitor all maintenance activities?	**Yes**
		MA-2.3				Is management's approval required for the removal of the information system or its components for off-site maintenance and repairs?	**N/A**
		MA-2.4				Do you check all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions? (E.g., verify that audit logs are still functioning properly, user level of access is still appropriate.)	**Yes**
	MA-5	MA-5.1	MAINTENANCE PERSONNEL	164.308(a)(3)(ii)(A) 164.310(a)(2)(iv)	A.9.4.5, A.11.2.4	Do you authorize and maintain a list of authorized maintenance personnel?	**Yes**
		MA-5.2				Do you ensure that personnel performing maintenance of the information system have the required access authorizations?	**Yes**
		MA-5.3				If personnel without the required access authorizations are allowed to perform maintenance activities (a vendor), are they supervised by authorized organizational personnel?	**Yes**

	MA-6	MA-6.1	TIMELY MAINTENANCE	164.310(a)(2)(iv)	A.11.2.4	Is there a maintenance contract with the vendor to provide timely maintenance in the event of a failure of the information system? (E.g., spare parts on hand, response times from the vendor or other personnel, documented in SLA agreements.)	**Yes**
Media Protection	MP-1	MP-1.1	MEDIA PROTECTION POLICY AND PROCEDURES	164.310(d)(1)	A.5.1.1, A.5.1.2, A.6.1.1, A.9.1.1, A.12.1.1, A.18.1.1, A.18.1.3, A.18.2.2	Is all removable media stored only on-site within a recognized data center?	**N/A**
		MP-1.2				Are there formally documented policies and procedures for Media Protection?	**N/A**
	MP-2	MP-2.1	MEDIA ACCESS	164.308(a)(3)(ii)(A), 164.310(c, 164.310(d)(1), 164.312(c)(1)	A.7.1.2, A.8.2.2, A.8.2.3, A.8.3.1, A.11.2.9	Is access to media associated with the information system (diskettes, hard disk drives, flash drives, CDs, paper, microfilm, etc.) restricted to authorized personnel?	**N/A**
	MP-3	MP-3.1	MEDIA MARKING	164.310(c , 164.310(d)(1)	A.7.1.2, A.8.2.2, A.8.2.3, A.8.3.1	Is any media containing sensitive data marked to indicate distribution limitations, handling caveats, ownership, and any applicable security markings if it is removed from a controlled area?	**N/A**
	MP-4	MP-4.1	MEDIA STORAGE	164.310(c, 164.310(d)(1), 164.310(d)(2)(iv)	A.8.2.3, A.8.3.1, A.11.2.9, A.18.1.3	Is the media stored is a secure location? (E.g., data center, locked office or cabinet.)	**N/A**
	MP-5	MP-5.1	MEDIA TRANSPORT	164.310(d)(1), 164.310(d)(2)(iii), 164.312(c)(1)	A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.5, A.11.2.6	Does media related to this information system get transported outside of the controlled environment?	**N/A**
		MP-5.2				Do you maintain accountability during the transport of the media outside of the controlled area, documenting transport activities and restricting transport activities to associated personnel?	**N/A**
	MP-6	MP-6.1	MEDIA SANITIZATION	164.310(d)(1), 164.310(d)(2)(i), 164.310(d)(2)(ii)	A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7	Is the media sanitized prior to destruction, disposal, re-use, or release? (I.e., degaussed.)	**N/A**
Physical and Environmental Protection	PE-1	PE-1.1	PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES	164.310(a)(1), 164.310(a)(2)(ii), 164.310(a)(2)(iii)	A.5.1.1, A.5.1.2, A.6.1.1, A.9.2.1, A.11.1.4, A.11.2.1, A.11.2.2, A.12.1.1, A.18.1.1, A.18.2.2	Are the servers and other equipment located within a certifed data center?	**Yes**
	PE-2	PE-2.1	PHYSICAL ACCESS AUTHORIZATIONS	164.310(a)(1), 164.310(a)(2)(iii)	A.9.2.1, A.9.2.5, A.11.1.2, A.11.1.5	Is there a documented and current list of personnel with authorized access to the facility where the information system resides?	**Yes**
		PE-2.2				Is the access list detailing the individuals with authorized facility access periodically reviewed?	**Yes**
		PE-2.3				Are individuals no longer requiring facility access removed from the list?	**Yes**
	PE-3	PE-3.1	PHYSICAL ACCESS CONTROL	164.310(a)(1), 164.310(a)(2)(iii), 164.310(b), 164.310(c	A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.5, A.11.1.6, A.11.2.8	Are there controls in place to verify individual access before granting access to the facility where the information system resides? (E.g., card readers.)	**Yes**
		PE-3.2				Do you maintain physical access audit logs for the necessary entry/exit points?	**Yes**
		PE-3.3				Are there any components of the information system available in a public area? (For example, a client on a public or publicly visible workstation.)	**No**
		PE-3.4				Do you escort visitors and monitor visitor activity?	**Yes**
		PE-3.5				Are physical access devices inventoried and periodically reviewed?	**Yes**
	PE-5	PE-5.1	ACCESS CONTROL FOR OUTPUT DEVICES	164.310(a)(1), 164.310(b), 164.310(c	A.11.1.2, A.11.1.3, A.11.2.8, A.13.1.1	Are monitors, printers, and audio devices physically secured so that unauthorized individuals may not obtain information from the output?	**Yes**
	PE-6	PE-6.1	MONITORING PHYSICAL ACCESS	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),	A.11.1.2, A.11.1.5, A.12.1.2	Is there monitoring of physical access to the facility where the information system resides to detect and respond to physical security incidents?	**Yes**
		PE-6.2				Are physical access logs reviewed?	**Yes**
		PE-6.3				Are the results of the review and investigation available for the incident response team?	**Yes**
	PE-17	PE-17.1	ALTERNATE WORK SITE	164.310(a)(2)(i)	A.6.2.2, A.11.2.6, A.13.2.1	In the event of an emergency, has an alternate work site with effective physical security controls been designated?	**Yes**
ing	PL-1	PL-1.1	SECURITY PLANNING POLICY AND PROCEDURES	164.316(a)	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2	Is there a security plan for this information system?	**Yes**
	PL-2	PL-2.1	SYSTEM SECURITY PLAN	164.310(a)(2)(ii), 164.316(a), 164.316(b)(1)	A.14.1.1	Does the security plan: - Explicitly define the authorization boundary for the system; - Describe the operational context of the information system in terms of missions and business processes;	**Yes**
		PL-2.2				Are copies of the security plan distributed and subsequent changes communicated to key personnel?	**Yes**
		PL-2.3				Is the security plan periodically reviewed?	**Yes**

Plann		PL-2.4				Is the plan updated to address changes in the environment?	**Yes**
		PL-2.5				Is the security plan protected from unauthorized disclosure and modification?	**Yes**
	PL-8	PL-8.1	INFORMATION SECURITY ARCHITECTURE	164.308(a)(1)(i), 164.308(a)(1)(ii)(A), 164.308(a)(3)(ii)(A), 164.308(a)(8), 164.310(d)	A.14.1.1	Does the organization have a comprehensive information security architecture for their information system?	**Yes**
		PL-8.2				Does the organization describe how the information security architecture is integrated into and supports the enterprise architecture?	**Yes**
		PL-8.3				Does the organization describe any information security assumptions and dependencies on external services?	**Yes**
Personnel Security	PS-1	PS-1.1	PERSONNEL SECURITY POLICY AND PROCEDURES	164.308(a)(3)(ii)(A), 164.308(a)(3)(ii)(B), 164.308(a)(3)(ii)C	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2	Are there formally documented policies and procedures for Personnel Security?	**Yes**
	PS-2	PS-2.1	POSITION CATEGORIZATION	164.308(a)(3)(ii)(B) 164.308(a)(1)(ii)(C), 164.308(a)(3)	A.6.1.1	Does the organization assign risk designations to all positions?	**Yes**
		PS-2.2				Does the organization establish screening criteria for individuals filling those positions?	**Yes**
		PS-2.3				Does the organization review and revise position risk designations at least every three years?	**Partial**
	PS-3	PS-3.1	PERSONNEL SCREENING	164.308(a)(3)(ii)(B)	A.7.1.1	Does the organization screen individuals prior to authorizing access to the information	**Yes**
	PS-4	PS-4.1	PERSONNEL TERMINATION	164.308(a)(3)(ii)(C)	A.7.3.1, A.9.2.6	Does the organization have appropriate termination procedures in place to those with access to the information system?	**Yes**
	PS-5	PS-5.1	PERSONNEL TRANSFER	164.308(a)(3)(ii)(C)	A.7.3.1, A.9.2.6	Does the organization have appropriate transfer procedures in place to those with access to the information system?	**Yes**
	PS-6	PS-6.1	ACCESS AGREEMENTS	164.308(a)(3)(ii)(A), 164.308(a)(3)(ii)(B), 164.308(a)(4)(ii)(B), 164.310(b), 164.310(d)(2)(iii), 164.314(a)(1), 164.314(a)(2)(i), 164.314(a)(2)(ii)	A.6.1.1, A.6.2.1, A.6.2.2, A.7.2.1, A.11.1.5, A.13.2.1, A.13.2.4	Does the organization have access agreements (reviewed annually) for individuals with access to the information system?	**Partial**
	PS-7	PS-7.1	THIRD-PARTY PERSONNEL SECURITY	164.308(a)(3)(ii)(A), 164.308(a)(4)(ii)(B), 164.308(b)(1), 164.314(a)(1), 164.314(a)(2)(i), 164.314(a)(2)(ii)	A.6.1.1, A.7.2.1, A.15.1.1, A.15.1.2	Does the organization have appropriate third-party access control procedures for external parties granted access to the information system?	**Yes**
	PS-8	PS-8.1	PERSONNEL SANCTIONS	164.308(a)(1)(ii)(C)	A.7.2.3	Does the organization have appropriate personnel sanctions policies and procedures?	**Yes**
Risk Assessment	RA-1	RA-1.1	RISK ASSESSMENT POLICY AND PROCEDURES	164.308(a)(1)(i), 164.316(a)	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2	Are there formally documented policies and procedures for Risk Assessments?	**Yes**
	RA-2	RA-2.1	SECURITY CATEGORIZATION	164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(7)(ii)(E	A.8.2.1	Does the organization categorize information and the information system in accordance with applicable Federal Laws, Executive Orders, directives, policies, regulations, standards and guidance?	**Yes**
	RA-3	RA-3.1	RISK ASSESSMENT	164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.316(a)	A.12.6.1, A.15.2.2, A.18.2.3	Does the organization conduct a risk assessment including the likelihood and impact of harm, from the unauthorized access, use, disclosure, disruption, modification or destruction of the information system and the information it processes, stores or transmits?	**Yes**
	RA-4	RA-4.1	VULNERABILITY SCANNING	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),	A.12.6.1, A.18.2.3	Does the organization scan for vulnerabilities in the information system and hosted applications and when new vulnerabilities potentially affecting the system/applications are identified and reported?	**Yes**
System and Services Acquisition	SA-4	SA-4.1	ACQUISITIONS	164.308(a)(1)(i), 164.308(a)(1)(ii)(D) 164.314(a)(2)(i)	A.14.1.1, A.14.2.7, A.14.2.9, A.15.1.2	Does the organization include the requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs	**Yes**
	SA-9	SA-9.1	EXTERNAL INFORMATION SYSTEM SERVICES	164.308(b)(1), 164.308(b)(4), 164.314(a)(1), 164.314(a)(2)(i), 164.314(a)(2)(ii)	A.6.1.1, A.6.1.5, A.7.2.1, A.11.2.5, A.11.2.6, A.13.1.2, A.13.2.2, A.13.2.4, A.14.2.7, A.15.1.1, A.15.1.2, A.15.2.1, A.15.2.2	Does the organization require that providers of external information system services comply with organizational information security requirements in accordance with applicable Federal Laws, Executive Orders, directives, policies, regulations, standards and guidance?	**Yes**

System and Communications Protection	SC-1	SC-1.1	SYSTEM AND COMMUNICATION PROTECTION POLICY AND PROCEDURE		A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2	Do you have formally documented policies and procedures for System and Communications Protection?	**Yes**
	SC-5	SC-5.1	DENIAL OF SERVICES OF PROTECTION	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),		Does the information system protect against or limits the effect of DOS/DDOS attacks?	**Partial**
	SC-7	SC-7.1	BOUNDARY PROTECTION	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),	A.12.1.2, A.12.2.1, A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3	Does the application/system monitor and control communications at the external boundary of the system and at key internal boundaries?	**Yes**
		SC-7.2				Does the system connect to other information systems only through managed interfaces, deny network traffic by default, and allow network traffic by exception (i.e., deny all, permit by exception)?	**Yes**
	SC-8	SC-8.1	TRANSMISSION CONFIDENTIALITY INTEGRITY	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),	A.8.2.3, A.10.1.1, A.13.1.1, A.13.1.2, A.13.2.1, A.13.2.2, A.13.2.3, A.14.1.2, A.14.1.3	Does the application/system protect the integrity of transmitted information?	**Yes**
		SC-8.2				Does the application/system employ cryptographic mechanisms to recognize changes to information during transmission (such as hashing algorithms)?	**Yes**
	SC-12	SC-12.1	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT	164.312(e)(2)(ii)	A.10.1.2	Are cryptographic keys established and managed?	**Yes**
	SC-13	SC-13.1	CRYPTOGRAPHY PROTECTION	164.308(a)(1)(ii)(D), 164.308(a)(3), 164.308(a)(4), 164.310(b), 164.310(c),	A.10.1.1, A.14.1.2, A.14.1.3, A.18.1.5	Does the information system use cryptographic protections for data-in-transit?	**Yes**
System and Information Integrity	SI-1	SI-1.1	SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES	164.312(c)(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	Do you have formally documented policies and procedures for System and Information Integrity?	**Partial**
	SI-3	SI-3.1	MALICIOUS CODE PROTECTION	164.306(e), 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B)	A.12.2.1	Do you have an anti-virus running with current updated virus definition (DAT) files?	**Yes**
		SI-3.2				Are the DAT files updated regularly?	**Yes**
		SI-3.3				Is the information system and its components periodically scanned for malicious code?	**Partial**
		SI-3.4				Are the administrators notified and do they respond to malicious code detections?	**Yes**
	SI-4	SI-4.1	INFORMATION SYSTEM MONITORING	164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B)	A.12.1.2, A.16.1.2, A.16.1.3	Is the information system monitored to detect attacks, potential attacks, and unauthorized use?	**Yes**
	SI-5	SI-5.1	SECURITY ALERTS, ADVISORIES, AND DIRECTIVES	164.308(a)(5)(ii)(A)	A.6.1.3, A.6.1.4, A.12.5.1, A.16.1.2, A.16.1.3	Does the team receive or subscribe to external security alerts, listservs, etc. related to the information system?	**Yes**
		SI-5.2				Does the team generate and disseminate internal security alerts, advisories, and directives as deemed necessary?	**Partial**
	SI-7	SI-7.1	SOFTWARE AND INFORMATION INTEGRITY	164.312(c)(1), 164.312(c)(2), 164.312(e)(2)(i)	A.12.2.1	Are integrity verification tools used to detect unauthorized changes to software, firmware, and information?	**Partial**
	SI-8	SI-8.1	SPAM PROTECTION	164.308(a)(5)(ii)(B)		Are spam protection mechanisms in place and updated as needed?	**Yes**