Centers for Medicare and Medicaid Services
Office of Enterprise Data and Analytics (OEDA)

7500 Security Boulevard
Baltimore, Maryland 21244-1850

Data Management Plan Self-Attestation Questionnaire (DMP SAQ):

Requirements & Guidance for Security & Privacy Controls

July 2025

CMS Data Privacy Safeguard Program
DPSP@cms.hhs.gov

Table of Contents

1. INTRODUCTION

The Centers for Medicare and Medicaid Services (CMS) are permitted to disclose certain types of CMS data to requesting research organizations for research purposes only. As part of the disclosure process, approved requesters enter into Data Use Agreements (DUAs) with CMS. The DUA outlines specific requirements to ensure that the disclosure of CMS data complies with CMS data release policies and related frameworks[1].

Specifically, the DUA states: "the DUA user is to establish appropriate administrative, technical, and physical safeguards to protect the confidentiality of data and to prevent unauthorized use or access to it." These safeguards must be aligned with security and privacy controls identified by the following frameworks:

- CMS *Acceptable Risk Safeguards* (ARS),Version 5.1x, and
- National Institute of Standards of Technology (NIST) Special Publication (SP) 800-53 Revision 5, *Security and Privacy Controls for Information Systems and Organizations*.

1.1 Scope

To properly identify if security and privacy controls have been implemented by the DUA organization, CMS requires the DUA organization to complete the evidence-based attestation questionnaire, now known as the *Data Management Plan Self-Attestation Questionnaire* (DMP SAQ). The DMP SAQ asks DUA organizations to attest that the organization complies with CMS ARS security and privacy controls imbedded within the questionnaire.

The DMP SAQ considers that information systems may vary between organizations and allows some flexibility in implementing compensating controls or alternative implementations. The important takeaway when implementing the controls is that the intent of security and privacy control is met. For any control that cannot be met, organizations must provide justification for not being able to implement the control.

1.2 Purpose

The purpose of *Requirements and Guidance for Security and Privacy Controls* is to:

1. Provide supplemental guidance on CMS ARS requirements for security and privacy controls,
2. Cross-reference the security and privacy control to the matching DMP SAQ question imbedded within the questionnaire, and
3. Spell out commonly used acronyms.

[1] Other relevant authorities to this Introduction include:

- Office of Management and Budget (OMB) Circular A-130, Appendix III--*Security of Federal Automated Information Systems*
- Federal Information Processing Standard (FIPS) 200, *Minimum Security Requirements for Federal Information and Information Systems"*
- The Privacy Act of 1974, §552
- Health Insurance Portability and Accountability Act (HIPAA) of 1996
- Federal Information Security Management Act (FISMA) of 2002

2. DPSP GUIDANCE FOR SECURITY AND PRIVACY CONTROLS

The CMS Data Privacy Safeguard Program (DPSP) has created the following CMS ARS control-specific guidance for interpretation and application for DUA organizations to use as they complete the DMP SAQ.

These controls are imbedded as attestation questions within the DMP SAQ, and this synthesized guidance is based on ARS and NIST control baselines, which serve as the starting point for organizations as they confirm that they have implemented the appropriate measures necessary to protect CMS data. Please note, the controls are presented by the control family identifiers and accordingly convey CMS policies.

For a complete list of all Control Requirement Structures, please visit CMS *Acceptable Risk Safeguards* (ARS), Version 5.1x.

A. SECURITY AND PRIVACY CONTROLS

1A. Access Controls: Attestation and Rationale

#	Question	Controls Reference
1.1	Does your organization have an access control policy that addresses the purpose, scope, responsibility, management commitment, coordination among organizational entities, and DUA compliance by all research parties using CMS data and is the policy disseminated to the appropriate personnel or roles? (ARS 5.1 AC-01)	ARS 5.1 AC-01 Guidance: Ensure that there is a documented access control policy that addresses the listed items. Rationale should include the name of the policy and how often the policy is reviewed or date of the last review as well as an outline or summary of the policy. Rationale should also include how the policy is disseminated to the appropriate personnel or roles.

#	Question	Controls Reference
1.2	Does your organization's account management system assign an account manager, ensure unique user accounts, ensure group/role conditions for membership, review user accounts periodically, and notify account managers within 30 days when accounts are no longer required or when system users are terminated or transferred? (ARS 5.1 AC-02)	ARS 5.1 AC-02 Guidance: Ensure access to the system is limited to authorized users, processes acting on behalf of authorized users, and devices (including other systems). Also, ensure access to the system is limited to the types of transactions and functions that authorized users are permitted to execute. Rationale should include an outline or summary of the account management or access control process or policy that addresses the following: a) Unique user accounts. b) Each user account has an account manager which is notified of changes. c) Group/role conditions for membership. d) Track account changes (e.g., creation, enabling, modifying, disabling, deletion) within audit records. e) Monitor user accounts. f) Review user accounts periodically. g) Centralized and automated account management.

#	Question	Controls Reference
1.3	Does your organization ensure it controls information flow within the system and any interconnected (internal or external) systems? Please describe where the information is coming from and where it is going. (ARS 5.1 AC-04)	ARS 5.1 AC-04 Guidance: Ensure the system controls the flow of information, particularly CMS data, in accordance with approved authorizations. Refer to network or data flow diagrams for the system, as needed. Rationale should include an outline of the safeguards implemented to restrict how, when, and to what devices or remote systems PII (to include PHI) or other sensitive data categorized as CUI are transmitted.
1.4	Does your organization have a process for approved information-sharing circumstances that determines what is shared with external users (e.g., collaborators) and ensures that access authorizations assigned to these users aligns with the organization's access restrictions? (ARS 5.1AC-21)	ARS 5.1 AC-21 Guidance: Ensure that there is a formal and/or administrative process for sharing CMS data with external users and ensure access to this data aligns with access restrictions employed by the organization for the system. Rationale should include information regarding a documented policy or process that indicates the security measures in place for sharing the agreed-upon information and outlines how external users are authorized, how they will access information, and expectations for adequately protecting the information.

1B. Access Controls: Attestation

#	Question	Controls Reference
1.5	Does your organization use logical access controls (e.g., roles, groups, file permissions) to restrict access to information? (ARS 5.1 AC-03)	ARS 5.1 AC-03 Guidance: Ensure the access control model is implemented and public read and write accesses are disabled to all system-related files, objects, and directories.
1.6	Does your organization's information system separate users based on their duties (e.g., users, researchers, management, etc.)? (ARS 5.1 AC-05)	ARS 5.1 AC-05 Guidance: Ensure the system separates the duties of users. No user should have access to complete system functionality.
1.7	Does your organization ensure that only authorized users have permissions required to perform their job functions by disabling non-essential functions and removable media devices; ensure security functions are explicitly authorized; ensure that authorized users utilize their own account to access the system; escalate privileges to perform administrative functions; and log all privileged account usage activities? (ARS 5.1 AC-06, AC-06(01), AC-06(09))	ARS 5.1 AC-06, AC-06(01), AC-06(09) Guidance: Ensure that users have the fewest permissions required to perform their job functions. Also: a) Disable all non-essential functions. b) Disable the use of removable media boot devices (e.g., thumb drives). c) Ensure security functions are explicitly authorized. d) Ensure that users utilize their own account to access system, then escalate privileges to perform administrative functions. e) Log all usage of privileged account activities.
1.8	Does your organization's information system automatically disable accounts after a defined number of consecutive failed login attempts? For systems that contain PII/PHI, when the limit of attempts is exceeded a system administrator intervention is required.	ARS 5.1 AC-07 Guidance: Ensure that the information system disables accounts after a number of consecutive failed login attempts.

#	Question	Controls Reference
	(ARS 5.1 AC-07)	For systems with PII/PHI, when the number of login attempts is exceeded, a system administrator should intervene to reactivate access.
1.9	Does your organization's information system display a notification or banner before granting access to the information systems? (ARS 5.1 AC-08)	ARS 5.1 AC-08 Guidance: Ensure the system displays a notification or banner before gaining access to the system which follows United States Government Configuration Baseline (USGCB) or other applicable guidelines. Require the user to take explicit action (e.g., clicking OK) to fully authenticate.
1.10	Does your organization's information system lock user devices after an organization defined time limit of inactivity and require the user to initiate a device lock before leaving the system unattended? Does it retain the device lock until the user reestablishes access using established identification and authentication procedures? (ARS 5.1 AC-11)	ARS 5.1 AC-11 Guidance: Ensure that users' devices lock after 15 minutes or other defined time limit for remote and internal sessions. Device locks shall block information on the screen. Ensure that user sessions are automatically disconnected under specified circumstances (e.g., extended period of inactivity, potentially malicious activity). Also, ensure that the device lock is retained until the user re-establishes access through identification and authentication procedures (i.e., username, passwords, or other credentialing.)
1.11	Does your organization identify actions (defined in applicable security and privacy plans) that can be taken on the system without identification or authentication (e.g., viewing certain webpages with public information only or generic information)? (ARS 5.1 AC-14)	ARS 5.1 AC-14 Guidance: Ensure the system defines what actions can be taken on the system without authentication (e.g., viewing certain webpages with public information). Note: If there are no actions that can be taken on the system without

#	Question	Controls Reference
		authentication, it is appropriate to respond “Yes”.
1.12	Does your organization’s remote connections have usage restrictions; connection requirements such as cryptography connected to managed network access control points; and have guidelines for user access? Are they monitored through audit record and explicitly authorize the usage of privileged commands through the remote connection? (ARS 5.1 AC-17, AC-17(01), AC-17(02), AC-17(03), AC-17(04))	ARS 5.1 AC-17, AC-17(01), AC-17(02), AC-17(03), AC-17(04) Guidance: Ensure that remote connections: a) Have usage restrictions. b) Have connection requirements such as cryptography and connected to managed network access control points. c) Have guidelines for user access. d) Are monitored through audit records. e) Explicitly authorizes the usage of privileged commands through the remote connection.
1.13	Does your organization establish configuration requirements, connection requirements, and implementation guidance for wireless access and/or mobile devices? (ARS 5.1 AC-18, AC-19)	ARS 5.1 AC-18, AC-19 Guidance: Ensure the system has usage restrictions and implementation guidance (e.g., encryption) for wireless access. Wireless access only includes direct internal wireless connections. Ensure the system has usage restrictions and implementation guidance (e.g., encryption of data at rest and data in transit) for mobile devices (e.g., tablets, cell phones) which have direct access to the system.
1.14	Does your organization ensure that the information system does not allow external systems to process, store, or transmit system information unless explicitly authorized? (ARS 5.1 AC-20, AC-20(01), AC-20(02))	ARS 5.1 AC-20, AC-20(01), AC-20(02) Guidance: Ensure that the system does not use systems outside of the authorization boundary to store, transmit, or view system information unless there is explicit authorization to do so. Restrict the

#	Question	Controls Reference
		usage of portable storage devices (e.g., thumb drives, external hard drives) which leave the information system boundary.
1.15	Does your organization have a process for determining what is shared with external users (e.g., collaborators)? (ARS 5.1 AC-21)	ARS 5.1 AC-21 Guidance: Ensure that the system has a process for determining what information on the system should be shared with external users. Note: This question is aligned with question 1.4.

2A. Awareness and Training Controls: Attestation and Rationale

#	Question	Controls Reference
2.1	Does your organization ensure that system users (including managers, senior executives, and contractors) receive security and privacy literacy training as part of initial training of new users, annually thereafter, and when required by system changes or events as defined by the organization; and that such users certify manually or electronically completion of training? (ARS 5.1 AT-02)	ARS 5.1 AT-02 Guidance: Ensure the system has a policy for completing security and privacy training. Ensure the system has a security and privacy training program which includes employees, contractors, managers, and senior staff. Training shall be completed before gaining access to the system and every 365 days. Follow CMS or organizational guidelines for training content. Ensure the training includes insider threat information. Users should also acknowledge training

		completion either via manual or electronic methods. Rationale should include excerpts from the policy, training materials, etc. or a summary of how implemented processes address all requirements outlined in the question.
2.2	Does your organization ensure that personnel are trained to carry out their assigned information security or privacy related duties and responsibilities prior to them assuming their security or privacy specific roles and responsibilities? Do they receive additional training based on system changes (e.g., statute, regulation, or policy changes) and at least once a year for refreshed role-based security and privacy training? (ARS 5.1 AT-03)	ARS 5.1 AT-03 Guidance: Ensure the system conducts role-based training (e.g., security-related, incident response, contingency planning) within 60 days of assuming the role and every 365 days. Rationale should include excerpts from the policy, training materials, etc. or a summary of how implemented processes address all requirements outlined in the question.

2B. Awareness and Training Controls

Please note that there are no questions in this section. Please proceed to 3A.

3A. Auditing and Accountability Controls: Attestation and Rationale

#	Question	Controls Reference
3.1	Does your organization have a policy for audit and accountability tasks to provide auditable evidence for system transactions on chance that an information system crashes, is hacked, or some other issue that disables the system and is the policy disseminated to the appropriate personnel or roles? (ARS 5.1 AU-01)	ARS 5.1 AU-01 Guidance: Ensure that there is a documented policy for audit and accountability tasks. Rationale should include the name of the policy and how often the policy is reviewed or date of the last review as well as an outline or summary of the policy. Rationale should also include how the policy is disseminated to the appropriate personnel or roles.

#	Question	Controls Reference
3.2	Does your organization's information system have the capability to log events in support of the audit function including: User logon and logoff (successful and unsuccessful), all system administration activities, modification of privileges and access, application alerts and error messages, configuration changes, account creation, modification or deletion, concurrent logon from different workstations, override of access control mechanisms, startup/shutdown of audit logging services, and audit logging service configuration changes? (ARS 5.1 AU-02)	ARS 5.1 AU-02 Guidance: Ensure that there is a system in place for auditing the listed event. Rationale should include excerpts from the policy, standard operating procedures, etc. or a summary of how implemented processes address all requirements outlined in the question. Rationale should include the system or tool used for auditing.
3.3	Does your organization ensure that the audit records from the information system contain the following metadata to support the detection, monitoring, investigation, response, and remediation of security and privacy incidents: Date and time of the event (e.g., timestamp); process identifier or system component (e.g., software, hardware) generating the event; user or account that initiated the event (unique username/identifier); event type; event outcome (success/failure); any privileged system functions executed; process creation information (command line captures if applicable)? (ARS 5.1 AU-03, AU-03(01))	ARS 5.1 AU-03, AU-03(01) Guidance: Ensure audit records contain the necessary metadata to support investigation and remediation of incidents. Rationale should include excerpts from the policy, standard operating procedures, etc. or a summary of how implemented processes address all requirements outlined in the question.

3B. Auditing and Accountability Controls: Attestation

#	Question	Controls Reference
3.4	Does your organization ensure adequate storage capacity to reduce the likelihood of such capacity being exceeded? (ARS 5.1 AU-04)	ARS 5.1 AU-04 Guidance: Ensure adequate storage capacity for audit records (recommended 90 days) or as required to reduce the likelihood of such capacity being exceeded.
3.5	Does your organization ensure that administrators are notified of process failures through the audit logging process of the information systems?	ARS 5.1 AU-05 Guidance: Ensure there is a standard operating procedure for handling audit system logging

#	Question	Controls Reference
	(ARS 5.1 AU-05)	processing failures or instances where audit storage capacity is exceeded without disabling auditing.
3.6	Does your organization ensure that: Audit records are reviewed weekly; system logs, network utilization/traffic, security software, and alerts are reviewed daily; automated audit record analysis is used to review audit records; automated audit record analysis is correlated across the organization; and administrator groups logs are inspected at least every 14 days to ensure unauthorized administrator, system, and privileged application accounts have not been created? (ARS 5.1 AU-06, AU-06(03))	ARS 5.1 AU-06, AU-06(03) Guidance: Ensure audit records are reviewed weekly or another recurring cadence. Use automated audit record analysis to review audit records. Correlate automated audit record analysis across the organization.
3.7	Does your organization ensure audit records are searchable? (ARS 5.1 AU-07(01))	ARS 5.1 AU-07(01) Guidance: Audit records shall be searchable to support monitoring and investigation of events or incidents.
3.8	Does your organization ensure the internal system clocks of the information systems are regularly synchronized with a common authoritative time source (e.g., atomic clocks, external NTP server, NIST time service, etc.) and that audit records use the internal system clocks to generate a time stamp? (ARS 5.1 AU-08)	ARS 5.1 AU-08 Guidance: Ensure internal system clocks are regularly synchronized with NIST time servers and that audit records use internal system clocks to generate a time stamp.
3.9	Does your organization ensure that audit information and audit logging tools are protected from unauthorized access, deletion, and modification? Is access to the management of audit logging functionality limited to a subset of privileged users? (ARS 5.1 AU-09, AU-09(04))	ARS 5.1 AU-09, AU-09(04) Guidance: Ensure audit records and tools are protected from unauthorized access, including encryption.
3.10	Does your organization ensure that audit records are retained for 90 days in “hot” storage and retained for one year in archive storage? (ARS 5.1 AU-11)	ARS 5.1 AU-11 Guidance: Retain audit records for 90 days in “hot” storage and archive storage for one year to support after-the-fact investigations. Comply with

#	Question	Controls Reference
		NARA requirements for storage.

4A. Assessment, Authorization, and Monitoring Controls: Attestation and Rationale

#	Question	Controls Reference
4.1	Does your organization have a policy for assessment, authorization, and monitoring activities that is reviewed/updated at least once a year or whenever there is a significant system modification and is the policy disseminated to the appropriate personnel or roles? (ARS 5.1 CA-01)	ARS 5.1 CA-01 Guidance: Ensure that there is a documented policy for assessment, authorization, and monitoring activities. Rationale should include the name of the policy and how often the policy is reviewed or date of the last review, an outline or summary of the policy. Rationale should also include how the policy is disseminated to the appropriate personnel or roles.
4.2	Does your organization approve and manage the exchange of information between the system and other systems where CMS data resides and document, as part of exchange agreements, the security and privacy requirements, controls, and responsibilities of each system? (ARS 5.1 CA-03, CA-09)	ARS 5.1 CA-03, CA-09 Guidance: Ensure that the organization manages the exchange of information: a) Using an Interconnection Security Agreement (ISA), information exchange security agreements, MOA, MOU, or service level agreement (SLA)*; b) Documenting interface, security requirements, and type of information exchanged within agreements; and c) Reviewing and updating agreements once per year or after a significant change *Exchange agreements are not necessary if the same IT infrastructure management is used.

#	Question	Controls Reference
		Rationale should include if there is any information exchange between systems and if so, what documentation is in place for information exchange.

4B. Assessment, Authorization, and Monitoring Controls: Attestation

#	Question	Controls Reference
4.3	Does your organization have a continuous monitoring program that manages identified vulnerabilities, remediation, and ongoing security and privacy assessments and reports the security and privacy status of the system to appropriate personnel or roles? (ARS 5.1 CA-07)	ARS 5.1 CA-07 Guidance: Ensure the system has a continuous monitoring program which monitors: a) Metrics related to identified vulnerabilities and remediation. b) Ongoing security and privacy assessments (DMP SAQ process counts as a security and privacy assessment). Also, ensure that the continuous monitoring program includes reporting the security and privacy status to appropriate personnel and roles.

5A. Configuration Management Controls: Attestation and Rationale

#	Question	Controls Reference
5.1	Does your organization have a policy for configuration management that is reviewed/updated at least once a year or whenever there is a significant system modification and is the policy disseminated to the appropriate personnel or roles? (ARS 5.1 CM-01)	ARS 5.1 CM-01 Guidance: Ensure that there is a documented policy for configuration management. Rationale should include the name of the policy and how often the policy is reviewed or date of the last review as well as an outline or summary of the policy. Rationale should also include how the policy is disseminated to the appropriate personnel or roles.
5.2	Does your organization track, review, approve or disapprove, and log changes to organizational information systems with explicit consideration for security and privacy impact analyses? (ARS 5.1 CM-03)	ARS 5.1 CM-03 Guidance: Ensure the system: a) Defines which changes to the system are controlled (i.e., requires approval) b) Reviews proposed changes with explicit attention to impact on security and privacy c) Documents and retains change control decisions for 3 years d) Periodically audits change control decisions e) Tests and validates change controls prior to implementation of the production system Rationale should include excerpts from the policy, standard operating procedures, etc. or a summary of how implemented processes address all requirements outlined in the question.
5.3	Does your organization establish and enforce security configuration settings for information technology products employed in the organizational information systems? (ARS 5.1 CM-06)	ARS 5.1 CM-06 Guidance: Ensure the system: a) Documents default configuration settings which

#	Question	Controls Reference
		follow the most restrictive mode possible for reliable operation b) Implements the configuration settings c) Documents any configuration deviations d) Monitors configuration changes e) Follows established configuration standards. Rationale should include excerpts from the policy, standard operating procedures, etc. or a summary of how implemented processes address all requirements outlined in the question.

5B. Configuration Management Controls: Attestation

#	Question	Controls Reference
5.4	Does your organization ensure that there is a current baseline configuration image for system components within the information system and review and update the baseline configuration at least once a year, when required due to major system changes/updates, or when system components are installed or upgraded? (ARS 5.1 CM-02)	ARS 5.1 CM-02 Guidance: Ensure the system has a current baseline configuration image for components within the system. Ensure the baseline configuration is reviewed and updated every 365 days or when a critical security patch is necessary. During system upgrades or installs which constitute a significant change, the baseline configuration shall be updated.
5.5	Does your organization ensure that the information system uses physical and logical access restrictions to prevent unauthorized changes to the information systems? (ARS 5.1 CM-05)	ARS 5.1 CM-05 Guidance: Ensure the system has physical and logical access restrictions in place to prevent unauthorizing changes. The organization should leverage implemented access and physical protection controls.

#	Question	Controls Reference
5.6	Does your organization ensure that the configuration of the information systems allows only essential functions, software, ports, protocols, and applications? (ARS 5.1 CM-07)	ARS 5.1 CM-07 Guidance: Ensure the system only allows essential functions, software, ports, protocols, and applications. Verify through monthly configuration scanning or automated mechanisms which provide enforcement.
5.7	Does your organization maintain and review at least every 180 days an up-to-date system inventory of metadata to include all boundary components, such as: Each component's unique identifier and/or serial number; the information system of which the component is a part; the type of information system component (e.g., server, desktop, application); the manufacturer/model information; the operating system type and version/service pack level; the presence of virtual machines; the application software version/license information; the physical location (e.g., building/room number); the logical location (e.g., IP address, position with the information system [IS] architecture); the media access control (MAC) address; ownership; operational status; primary and secondary administrators; and primary use? (ARS 5.1 CM-08, CM-08(01))	ARS 5.1 CM-08, CM-08(01) Guidance: Ensure the system maintains an up-to-date system inventory which includes all components within the computing environment hosting CMS data. Metadata shall include the listed items to the greatest extent possible.
5.8	Does your organization ensure that the information system prevents users from installing non-approved software through user policies? (ARS 5.1 CM-11)	ARS 5.1 CM-11 Guidance: Ensure the system prevents users from installing software through user policies. Monitor the installation of software on the system.

6A. Contingency Planning Controls: Attestation and Rationale

#	Question	Controls Reference
6.1	Does your organization have a policy for contingency planning that is reviewed/updated at least once a year or	ARS 5.1 CP-01, CP-02(01)

#	Question	Controls Reference
	when there is a significant system modification and is the policy disseminated to the appropriate personnel or roles? Does your organization's contingency planning include coordination with organizational elements responsible for related plans (e.g., Business Continuity Plans, Disaster Recovery Plans, Critical Infrastructure Plans, Continuity of Operations Plans, etc.)? (ARS 5.1 CP-01, CP-02(01))	Guidance: Ensure that there is a documented policy for contingency planning that coordinates with other organizational elements responsible for related plans. Rationale should include the name of the policy and how often the policy is reviewed or date of the last review. Rationale should also include how the policy is disseminated to the appropriate personnel or roles.
6.2	Does your organization perform full weekly and incremental daily backups of user-level information, system-level information, and information system documentation including security and privacy related documentation? How does your organization protect the confidentiality, integrity, and availability of backups containing CMS data? (ARS 5.1 CP-09)	ARS 5.1 CP-09 Guidance: Ensure the system performs full weekly and incremental daily backups of: a) User level data b) System data c) System documentation Also, ensure that the system protects the confidentiality, integrity, and availability of backups containing CMS data. Rationale should include processes related to backups and if CMS data is included in backup processes. If CMS data is included, the rationale should include where backups are located. Backup locations with CMS data should be considered as part of the computing environment.

6B. Contingency Planning Controls: Attestation

Please note that there are no questions in this section. Please proceed to 7A.

7A. Identification and Authentication Controls: Attestation and Rationale

#	Question	Controls Reference
7.1	Does your organization have a policy for identification and authentication that is reviewed/updated at least once a year or when there is a significant system modification and is the policy disseminated to the appropriate personnel or roles? (ARS 5.1 IA-01)	ARS 5.1 IA-01 Guidance: Ensure that there is a documented identification and authentication policy. Rationale should include the name of the policy and how often the policy is reviewed or date of the last review, as well as an outline or summary of the policy. Rationale should also include how the policy is disseminated to the appropriate personnel or roles.
7.2	Does your organization uniquely identify and authenticate users, processes, or devices prior to granting access to organizational systems through effective identity proofing and authentication processes? Describe how your organization establishes initial content for authenticators; defines reuse conditions; and sets minimum and maximum lifetimes for each authenticator type to be used. (ARS 5.1 IA-02, IA-03, IA-05, IA-12)	ARS 5.1 IA-02, IA-03, IA-05, IA-12 Guidance: Ensure the system: a) Verifies that the correct identifier is being issued to a person or device during authenticator distribution b) Has a standard for authenticator schema (e.g. first initial, last name, number, if duplicate) c) Meets or exceeds enforcement of established password complexity requirements. 1. If the operating environment enforces a minimum number of changed characters when new passwords are created, set the value commensurate with security categorization of the system. d) Stores and transmits only encrypted representations of passwords; and e) Allows the use of a temporary password for system logons

#	Question	Controls Reference
		with an immediate change to a permanent password f) Employs identify proofing processes Rationale should include excerpts from the policy, standard operating procedures, etc. or a summary of how implemented processes address all requirements outlined in the question.

7B. Identification and Authentication Controls: Attestation

#	Question	Controls Reference
7.3	Does your organization's information system use unique identifiers for users and scheduled processes (e.g., backups)? (ARS 5.1 IA-02)	ARS 5.1 IA-02 Guidance: Ensure the system uses unique identifiers for users and scheduled processes (e.g., backups).
7.4	Does your organization ensure the information system uniquely identifies devices (e.g., IP address, hostname, etc.)? (ARS 5.1 IA-03)	ARS 5.1 IA-03 Guidance: Ensure the system uniquely identifies devices (e.g., IP address, hostname).
7.5	Does your organization successfully assign unique identifiers to users and devices; prevent reuse of identifiers for three years or verify that access to sensitive information is removed prior to any reuse; and disable identifiers after 60 days of inactivity? (ARS 5.1 IA-04)	ARS 5.1 IA-04 Guidance: Ensure the system successfully assigns unique identifiers to users and devices, does not reuse identifiers for 3 years, and disables inactive identifiers after 60 days (or other acceptably defined period) of inactivity. Do not use PII as part of an identifier.
7.6	Does your organization ensure the information system shows non-descript information when authentication fails?	ARS 5.1 IA-06

#	Question	Controls Reference
	(ARS 5.1 IA-06)	Guidance: Ensure the system shows non-descript information upon failed login to protect authentication information from potential misuse. Authentication information should also be obscured during the authentication process.

8A. Incident Response Controls: Attestation and Rationale

#	Question	Controls Reference
8.1	Does your organization have an incident response policy that is reviewed/updated at least once a year or when there is a significant system modification and is the policy disseminated to the appropriate personnel or roles? (ARS 5.1 IR-01)	ARS 5.1 IR-01 Guidance: Ensure that there is a documented incident response policy. Rationale should include the name of the policy and how often the policy is reviewed or date of the last review as well as an outline or summary of the policy. Rationale should also include how the policy is disseminated to the appropriate personnel or roles.
8.2	Does your organization investigate incidents (e.g., preparation, detection, analysis, containment, eradication, and recovery); consistently track and monitor incidents (e.g., physical, technical, and privacy); and ensure that the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization? Describe how your organization investigates incidents. (ARS 5.1 IR-04, IR-05)	ARS 5.1 IR-04, IR-05 Guidance: Ensure the organization can investigate security incidents, to include preparation, detection, analysis, containment, eradication, and recovery. Ensure the system tracks security incidents (e.g., physical, technical, and privacy). Ensure that the system requires

#	Question	Controls Reference
		personnel to report potential incidents and investigate the potential incident. Rationale should include excerpts from the policy, standard operating procedures, etc. or a summary of how implemented processes address all the requirements outlined in the question.
8.3	With regard to data breaches, can your organization attest that there have been no breaches affecting 500 or more data subjects reported to the HHS Office for Civil Rights within the last 2 years? If there has been a breach, please provide the nature and date of the breach. (ARS 5.1 IR-08(01))	ARS 5.1 IR-08(01) Guidance: Ensure that if your organization has had a breach meeting the parameters outlined, that it is properly documented and reported.

8B. Incident Response Controls: Attestation

#	Question	Controls Reference
8.4	Does your organization ensure that employees who have incident response duties complete incident response training within one month of assuming the role and annually thereafter and that incident response training content is reviewed and updated annually? (ARS 5.1 IR-02)	ARS 5.1 IR-02 Guidance: Ensure that employees who have incident response duties complete incident response training with one month of assuming the role and every 365 days. Review and update training content every 365 days.
8.5	Does your organization have the capability to investigate incidents (e.g., physical, technical and privacy), that includes preparation, detection, analysis, containment, eradication, and recovery and ensure that the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization? (ARS 5.1 IR-04, IR-05)	ARS 5.1 IR-04, IR-05 Guidance: Ensure the system can investigate security incidents, including preparation, detection, analysis, containment, eradication, and recovery.

#	Question	Controls Reference
8.6	Does your organization have incident response resources that can assist system administrators (e.g., help desks, assistance groups, access to forensics services, etc.) for the handling and reporting of security and privacy incidents? (ARS 5.1 IR-07)	ARS 5.1 IR-07 Guidance: Ensure the system has an incident response resource which can assist system administrator (and users) with the handling and reporting of incidents.
8.7	Does your organization have an incident response plan that: Provides the organization with a roadmap for implementing its incident response capability; describes the structure and organization of the incident response capability; provides a high-level approach for how the incident response capability fits into the overall organization; meets the unique requirements of the organization, which relate to mission, size, structure, and functions; defines reportable incidents; provides metrics for measuring the incident response capability within the organization; defines the resources and management support needed to effectively maintain and mature an incident response capability; is reviewed and approved by the applicable Incident Response Team Leader; is distributed to the organization's information security officers and other incident response team personnel; is reviewed within every 365 days or when an IR event(s) demonstrates a change and/or update is needed to improve the IR Plan; is updated to address system/organizational changes or problems encountered during plan implementation, execution, or testing; communicate incident response plan changes to the organizational elements listed above; and is protected from unauthorized disclosure and modification? (ARS 5.1 IR-08)	ARS 5.1 IR-08 Guidance: Ensure the system has an incident response plan which includes the essential elements and requirements for the organization's incident response capability to the greatest extent possible. The incident response plan should be a structured plan for handling incidents, including preparation, detection, response, and recovery.
8.8	Does your organization include in the incident response plan for breaches involving PII/PHI: A process to determine if notice to individuals or other organizations, including oversight organizations, is needed; an assessment process to determine the extent of harm, embarrassment, inconvenience, or unfairness to affected individuals and any mechanisms to mitigate such harms; and identification of any applicable privacy requirements. (ARS 5.1 IR-08(01))	ARS 5.1 IR-08(01) Guidance: Ensure that the organization includes in the incident response for breaches involving PII/PHI: a) Processes to determine if notice to individuals or other organizations, including oversight organizations, is needed

#	Question	Controls Reference
		b) An assessment process to determine the extent of harm, embarrassment, inconvenience, or unfairness to affected individuals and any mechanisms to mitigate such harms; and c) Identification of any applicable privacy requirements. The incident response plan should include how organizations handle breaches involving PII/PHI.

9A. Maintenance Controls: Attestation and Rationale

Please note that there are no questions in this section. Please proceed to 9B.

9B. Maintenance Controls: Attestation

#	Question	Controls Reference
9.1	Does your organization have a system maintenance policy that is reviewed/updated at least once a year or when there is a significant system modification and is the policy disseminated to the appropriate personnel or roles? (ARS 5.1 MA-01)	ARS 5.1 MA-01 Guidance: Ensure that there is a documented system maintenance policy that is reviewed/updated annually or when there is a significant change to the system. Ensure that the policy is disseminated to the appropriate personnel or roles.
9.2	Does your organization ensure it is not utilizing diagnostic hardware, software, or firmware maintenance tools that have been improperly modified within the data center? (ARS 5.1 MA-03, MA-03(01))	ARS 5.1 MA-03, MA-03(01) Guidance: Ensure the system utilizes diagnostic hardware, software, or firmware maintenance tools within the data center (or computing environment) that have not been improperly modified. Tools

		involved in system maintenance, if applicable, should be approved and monitored during usage.
9.3	Does your organization check media containing diagnostic and test programs being introduced into the system for malicious code, where applicable? (ARS 5.1 MA-03(02))	ARS 5.1 MA-03(02) Guidance: Ensure the system checks media containing diagnostic and test programs being introduced into the system for malicious code.

10A. Media Protection Controls: Attestation and Rationale

#	Question	Controls Reference
10.1	Does your organization have a media protection policy that is reviewed/updated at least once a year or when there is a significant system modification and is the policy disseminated to the appropriate personnel or roles? (ARS 5.1 MP-01)	ARS 5.1 MP-01 Guidance: Ensure that there is a documented policy for media protection. Rationale should include the name of the policy and how often the policy is reviewed or date of the last review as well as an outline or summary of the policy. Rationale should also include how the policy is disseminated to the appropriate personnel or roles.
10.2	Does your organization prohibit the use of personally owned storage media? (ARS 5.1 MP-07)	ARS 5.1 MP-07 Guidance: Ensure the system prohibits the use of personally owned media.

#	Question	Controls Reference
		Rationale should include how the organization prohibits the use of personally owned storage media, or if such media is allowed, how the organization ensures that users are restricted from uploading sensitive data to personally owned devices.
10.3	Does your organization ensure that any allowed portable storage devices have an identified owner (e.g., designated personnel or organization)? (ARS 5.1 MP-07)	ARS 5.1 MP-07 Guidance: Ensure any allowed portable storage devices have an identified owner. Rationale should include how the organization ensures that any allowed portable storage devices have an identified owner whether it is designated personnel, organization, or otherwise. There should still be restrictions around uploading sensitive data to portable devices.
10.4	Does your organization protect and securely store digital media and ensure that any media with CMS data (including backups) is disposed of (e.g., clearing, purging, or destroying) in accordance with standards and policies, such as the latest revision of NIST SP 800-88, when such data is no longer required? (ARS 5.1 MP-04, MP-06)	ARS 5.1 MP-04, MP-06 Guidance: Ensure the organization securely stores digital media and ensures that any media with CMS data is properly disposed of in accordance with standards and policies when such data is no longer required for the purpose of the project or study or when CMS data is transferred to an approved computing environment. Rationale should include how the organization securely stores digital media to include media received by CMS and what mechanisms are in place to properly dispose of media with CMS data when the data is no longer required.

10B. Media Protection Controls: Attestation

#	Question	Controls Reference
10.5	Does your organization ensure the information system administrators mark system media based on the classification of information the media holds? (ARS 5.1 MP-03)	ARS 5.1 MP-03 Guidance: Ensure the organization marks system media based on the classification of information the media holds. If system media is not used, ensure the organization has a process to classify system media based on an established classification system.
10.6	Does your organization protect media: While being transported, to include hand-carried – uses a securable container (e.g., locked briefcase) via authorized personnel; shipped – tracks with receipt by commercial carrier; maintains accountability for information system media during transport outside of controlled areas; documents activities associated with the transport of information system media; and restricts the activities associated with the transport of information system media to authorized personnel? (ARS 5.1 MP-05)	ARS 5.1 MP-05 Guidance: Ensure the system protects system media while being transported. This includes: a) If hand carried, using a securable container (e.g., locked briefcase) via authorized personnel b) If shipped, trackable with receipt by commercial carrier c) Maintains accountability for information system media during transport outside of controlled areas; d) Documents activities associated with the transport of information system media; and e) Restricts the activities associated with the transport of information system media to authorized personnel. Note: This control is mainly for any system media used within the organization that does not have CMS data or for approved activities involving the transport of CMS data. CMS data should

#	Question	Controls Reference
		not be physically transported once received.
10.7	Does your organization sanitize media prior to disposal or reuse and track such activities? (ARS 5.1 MP-06, MP-06(01))	ARS 5.1 MP-06, MP-06(01) Guidance: Ensure the system sanitizes media prior to disposal or reuse and tracks such activities. Sanitization processes should be in line with best practices for media disposition.

11A. Physical and Environmental Controls: Attestation and Rationale

Please note that there are no questions in this section. Please proceed to 11b.

11B. Physical and Environmental Controls: Attestation

#	Question	Controls Reference
11.1	Does your organization have a physical and environmental policy that is reviewed/updated at least once a year or when there is a significant system modification and is the policy disseminated to the appropriate personnel or roles? (ARS 5.1 PE-01)	ARS 5.1 PE-01 Guidance: Ensure that there is a documented physical and environmental policy that is reviewed/updated annually or when there is a significant change to the system. Ensure that the policy is disseminated to the appropriate personnel or roles.
11.2	Does your organization maintain a current list of authorized individuals to enter the facility? (ARS 5.1 PE-02)	ARS 5.1 PE-02 Guidance: Ensure the system maintains a current list of

#	Question	Controls Reference
		authorized individuals to enter the facility. Note: For computing environments using Cloud Service Providers (CSPs), organizations should have physical controls in place for the location where media with CMS data is stored and/or endpoints accessing CMS are located.
11.3	Does your organization ensure it: Verifies individual access authorizations before granting access to the facility; controls ingress/egress to the facility using guards and/or defined physical access control systems/devices (defined in the applicable security plan); maintains physical access audit logs for defined entry/exit points (defined in the applicable security plan); provides defined security safeguards (defined in the applicable security plan) to control access to areas within the facility officially designated as publicly accessible; escorts visitors and monitors visitor activity in defined circumstances requiring visitor escorts and monitoring (defined in the applicable security plan); secures keys, combinations, and other physical access devices; inventories defined physical access devices (defined in the applicable security plan), no less often than every (90 High, 90 Moderate, or 180 Low) days; and changes combinations and keys for defined high-risk entry/exit points (defined in the applicable security plan) every 365 days, and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated? (ARS 5.1 PE-03)	ARS 5.1 PE-03 Guidance: Ensure that the organization implements the listed physical access controls to the greatest extent possible. Note: For computing environments using Cloud Service Providers (CSPs), organizations should have physical controls in place for the location where media with CMS data is stored and/or endpoints accessing CMS are located.
11.4	Does your organization ensure that telephone and network hardware and transmission lines are protected? (ARS 5.1 PE-04)	ARS 5.1 PE-04 Guidance: Ensure that the organization controls physical access to telephone and network hardware and transmission lines. Note: For computing environments using Cloud Service Providers (CSPs), organizations should have

#	Question	Controls Reference
		physical controls in place for the location where media with CMS data is stored and/or endpoints accessing CMS are located.
11.5	Does your organization ensure that all unused physical ports (e.g., wiring closets, patch panels, etc.) are physically or logically disabled, locked, or barred? (ARS 5.1 PE-04)	ARS 5.1 PE-04 Guidance: Ensure that unused physical ports (e.g., wiring closets, patch panels, etc.) are disabled, locked, barred, or otherwise physically protected. Note: For computing environments using Cloud Service Providers (CSPs), organizations should have physical controls in place for the location where media with CMS data is stored and/or endpoints accessing CMS are located.

12A. Planning Controls: Attestation and Rationale

#	Question	Controls Reference
12.1	Does your organization have a complete and up-to-date system security and privacy plan? How often is it reviewed/updated? Is it reviewed/updated to address changes to the information system and environment of operation? (ARS 5.1 PL-02)	ARS 5.1 PL-02 Guidance: Ensure the system has a complete and up-to-date system security and privacy plan which includes the required and necessary information. Rationale should include the name of the plan or attestation that a plan exists and how often the plan is reviewed or date of the last review.

#	Question	Controls Reference
		Note: Security and privacy plans can be in the form of overarching information system security and privacy policies or procedures. A plan can also be a collection of policy or procedure documentation.
12.2	Does your organization ensure that rules of behavior (e.g., user agreements, system use agreements, etc.) describe the responsibilities and expected behavior for information system usage, security and privacy and are signed by all users and administrators? Is this updated/reviewed at least once a year? How is it acknowledged? (ARS 5.1 PL-04)	ARS 5.1 PL-04 Guidance: Ensure that all users and system administrators sign rules of behavior. Rationale should include what is required for users and administrators to sign, how often it is reviewed and updated, and how any rules of behavior are acknowledged (whether manually or electronically) by users and system administrators.

12B. Planning Controls: Attestation

Please note that there are no questions in this section. Please proceed to 13A.

13A. Personnel Security Controls: Attestation and Rationale

Please note that there are no questions in this section. Please proceed to 13B.

13B. Personnel Security Controls: Attestation

#	Question	Controls Reference
13.1	Does your organization follow organizational policy regarding background checks and screening for employees with access to CMS data? (ARS 5.1 PS-03)	ARS 5.1 PS-03 Guidance: Ensure the system follows organizational policy regarding background checks and

#	Question	Controls Reference
		screening for employees with access to CMS data.
13.2	Does your organization upon termination of individual employment: Disable information system access before or during termination; terminate/revoke any authenticators/credentials associated with the individual; conduct exit interviews that include a discussion of non-disclosure of information security and privacy information; retrieve all security-related organizational information system-related property; retain access to organizational information and information systems formerly controlled by the terminated individual; notify defined personnel or roles (defined in the applicable security plan) within one calendar day; and immediately escort employees terminated for cause out of the organization? (ARS 5.1 PS-04)	ARS 5.1 PS-04 Guidance: Ensure that employee termination processes follow the outlined steps. If any of the outlined steps are not followed, please indicate the step that is not implemented and the rationale for not implementing this step. If there are any processes that are followed but not included in the outlined list, please provide this information within the rationale.
13.3	Does your organization have processes for re-screening personnel according to organizationally defined conditions as required? (ARS 5.1 PS-03)	ARS 5.1 PS-03 Guidance: Ensure that the organization has established procedures for re-screening personnel consistent with the sensitivity risk designation of the position and organizational policy. If re-screening is not required, please indicate how the organization ensures personnel accessing CMS data maintain the proper trustworthiness and authorizations.
13.4	Does your organization ensure that users sign access agreements every 365 days? (ARS 5.1 PS-06)	ARS 5.1 PS-06 Guidance: Ensure that users sign access agreements every 365 days. If users are not required annually, please indicate under what circumstances users are required to re-review and sign access agreements.

#	Question	Controls Reference
13.5	Does your organization ensure that third-party service providers (contractors, CSPs, vendor maintenance) follow the same personnel requirements as full-time employees? (ARS 5.1 PS-07)	ARS 5.1 PS-07 Guidance: Ensure that third-party service providers (contractors, CSPs, vendor maintenance) follow the same personnel requirements as full-time employees. If third-party service providers are not utilized, the organization must ensure there are processes in place for external personnel security.
13.6	Does your organization ensure that the organization has a formal sanction process for employees who violate security policies or procedures? (ARS 5.1 PS-08)	ARS 5.1 PS-08 Guidance: Ensure the system has a formal sanction process for employees who violate security policies or procedures. Processes should be documented, reflect applicable laws and regulations, and include notification to the sanctioned individuals.

14A. Risk Assessment Controls: Attestation and Rationale

#	Question	Controls Reference
14.1	Does your organization utilize an automated vulnerability scanner in compliance with organizational policies? How is this performed? (ARS 5.1 RA-05)	ARS 5.1 RA-05 Guidance: Ensure the system utilizes an automated vulnerability scanner which complies with organizational

		policies. Scans should be running once every 72 hours or when a new threat has been discovered. Remediation shall also comply with organizational policies. Scans must be authenticated as a privileged user. Rationale should include what systems or tools are used for scanning, how scanning is performed, and how often.

14B. Risk Assessment Controls: Attestation

Please note that there are no questions in this section. Please proceed to 15A.

15A. System and Services Acquisition Controls: Attestation and Rationale

Please note that there are no questions in this section. Please proceed to 15B.

15B. System and Services Acquisition Controls: Attestation

#	Question	Controls Reference
15.1	Does your organization obtain or develop administrator documentation for the system or system components that describes: Secure configuration, installation, or operation; effective use and maintenance of security and privacy functions and mechanisms; and known vulnerabilities regarding configuration and use of administrative or privileged functions? (ARS 5.1 SA-05)	ARS 5.1 SA-05 Guidance: Ensure the system obtains or develops administrator documentation for the system or system components, to include: a) Secure configuration, installation, or operation; b) Effective use and maintenance of security and privacy functions and mechanisms; and c) Known vulnerabilities regarding configuration and use of administrative or privileged functions
15.2	Does your organization acquire, develop, and manage the system using a system development life cycle (SDLC) process that incorporates information security and privacy	ARS 5.1 SA-03, SA-08 Guidance: Organizations should acquire, develop, and manage

	considerations as well as apply security and privacy engineering principles in specification, design, development, implementation, and modification of the system and system components? (ARS 5.1 SA-03, SA-08)	systems within the computing environment using a system development life cycle (SDLC) process, where applicable.
15.3	Does your organization ensure that any external system services (third-party tools for ticketing, messaging, auditing, monitoring, etc.) outside of the system boundary comply with organizational information security and privacy requirements? (ARS 5.1 SA-09)	ARS 5.1 SA-09 Guidance: Ensure that providers of any external system services that are not part of the computing environment comply with organizational information security and privacy requirements.

16A. System and Communications Protection Controls: Attestation and Rationale

#	Question	Controls Reference
16.1	Does your organization monitor, control, and protect communications (e.g., information transmitted or received by organizational systems) at the external interfaces and key internal interfaces of organizational systems? What type of system is used? (ARS 5.1 SC-07)	ARS 5.1 SC-07 Guidance: Ensure the system has boundary protection (e.g., firewall, IDS/IPS). Boundary protection mechanisms: a) Must operate on a deny-all, permit-by-exception principle b) Must utilize stateful inspection mechanisms c) Must utilize 2 different vendors for boundary protection, where feasible If the system has a public component, web traffic coming into the system must have malware detection and monitoring of traffic which is sent into the organizations SIEM as defined within audit and accountability controls. Logs from devices must be sent to the

#	Question	Controls Reference
		organizations SIEM as defined within audit and accountability. Rationale should include the types of boundary protection that are in place and what systems or tools are employed in the computing environment for monitoring, controlling, and protecting network traffic communications.
16.2	Does your organization ensure that the information systems use FIPS 140-2 validated cryptographic modules for transmission of data-in-motion and/or data-at-rest? (FIPS 140-2, ARS 5.1 SC-08, SC-13, SC-28)	FIPS 140-2, ARS 5.1 SC-08, SC-13, SC-28 Guidance: Ensure the system uses FIPS 140-2 validated cryptographic modules for transmission of data and for protecting data at rest. If FIPS 140-2 is not feasible, organizations should implement the most robust encryption mechanisms possible. Rationale should include what is employed for encryption for transmission of data and for protecting data at rest and should indicate whether FIPS 140-2 validated modules are used.

16B. System and Communications Protection Controls: Attestation

#	Question	Controls Reference
16.3	Does your organization ensure that administrative and regular user interfaces are separate? (ARS 5.1 SC-02)	ARS 5.1 SC-02 Guidance: Ensure that administrative and regular user interfaces are separate.

#	Question	Controls Reference
16.4	Does your organization's information system deny network communications traffic by default and allow network communications traffic by exception at managed interfaces or for specific systems? (ARS 5.1 SC-07(05))	ARS 5.1 SC-07(05) Guidance: Ensure the system uses a deny-all, permit-by-exception policy for system access and network traffic.
16.5	Does your organization ensure that the information system terminates the network connection associated with a communications session at the end of the session or after a defined period of inactivity? (ARS 5.1 SC-10)	ARS 5.1 SC-10 Guidance: Ensure that the system can terminate a network connection at the end of communication sessions or automatically disconnects after a defined period activity. Examples include, but are not limited to, Dynamic Host Configuration Protocol (DHCP) sessions or VPN connections.
16.6	Does your organization have a centralized cryptographic key management system that complies with organizational standards? (ARS 5.1 SC-12)	ARS 5.1 SC-12 Guidance: Ensure the system has a cryptographic key management system which complies with organizational standards. Organizations that do not employ centralized key management systems should indicate whether cryptographic keys are managed locally or through some other means.
16.7	Does your organization prohibit collaborative computing mechanisms (e.g., networked white boards, cameras, microphones, etc.) unless explicitly authorized? (ARS 5.1 SC-15)	ARS 5.1 SC-15 Guidance: Ensure the system prohibits collaborative computing mechanisms (e.g., networked white boards, cameras, microphones, etc.) unless explicitly authorized. If authorized, ensure that the system prohibits remote activation of devices.

17A. System and Information Integrity Controls: Attestation and Rationale

#	Question	Controls Reference
17.1	Does your organization update malicious code protection mechanisms when new releases are available and perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed? (ARS 5.1 SI-03)	ARS 5.1 SI-03 Guidance: Ensure the system uses malicious code protection which: a) Has up-to-date virus definitions b) Scans important file systems every 12 hours and full system every 72 hours Rationale should include information regarding what malicious code protection mechanisms are in place and how scanning of malicious code is performed.
17.2	Does your organization monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks? Is the monitoring used to identify unauthorized use of organizational systems? (ARS 5.1 SI-04, SI-04(04))	ARS 5.1 SI-04, SI-04(04) Guidance: Ensure the system uses intrusion detection systems or intrusion protection systems (IDS/IPS) to monitor network communication. Both must be capable of decrypting network traffic. Ensure inbound and outbound communication is monitored. Rationale should include what is in place for monitoring inbound and outbound communications traffic and whether monitoring is in place to identify unauthorized use of the system.
17.3	Does your organization use file integrity monitoring (FIM) through employing tools and capabilities to monitor changes to critical resources such as operating system software components (e.g., OS images, kernel drivers, daemons), system firmware (e.g., the basic input/output system [BIOS]), and vital applications? (ARS 5.1 SI-07)	ARS 5.1 SI-07 Guidance: Ensure the system uses file integrity monitoring to monitor changes to critical system files, configurations, or data. Rationale should include information regarding what systems or tools are in place for

#	Question	Controls Reference
		monitoring changes to files and systems to detect suspicious activity or unauthorized tampering. If file integrity monitoring is not employed, rationale should include if there are any compensating controls such as enhanced monitoring and logging or manual processes.

17B. System and Information Integrity Controls: Attestation

#	Question	Controls Reference
17.4	Does your organization's information system: Identify system flaws; test updates prior to installation on production systems; correct high/critical security-related system flaws within 10 business days on production servers and 30 days on non-production servers; centrally manage flaw remediation; and track and approve any security-related patches which are not installed? (ARS 5.1 SI-02)	ARS 5.1 SI-02 Guidance: Ensure the system: a) Identifies system flaws b) Test updates prior to installation on production systems c) Corrects security-related system flaws within 10 business days on production servers, 30 days on non-production servers d) Centrally manage flaw remediation e) Track and approve any security-related patches which are not installed. Organizations with alternative implementations around identifying and correcting system flaws should provide rationale that speaks to what is employed.
17.5	Does your organization's information system use malicious code protection that has up-to-date virus definitions and scans important file systems every 12 hours and full system every 72 hours? (ARS 5.1 SI-03)	ARS 5.1 SI-03 Guidance: Ensure the system uses malicious code protection which: a) Has up to date virus definitions

#	Question	Controls Reference
		b) Scans important file systems every 12 hours and full system every 72 hours
17.6	Does your organization employ spam filters for email servers hosted within the system boundary, if applicable? (ARS 5.1 SI-08)	ARS 5.1 SI-08 Guidance: If the system has an email server, ensure that spam protection is used. Note: If e-mail servers are not part of the computing environment, organizations should respond "Yes" and provide rationale that there are no email servers in the environment.
17.7	Does your organization's information system validate user input (e.g., username, password, or data entry fields) before accepting it into the system to protect against injection attacks, cross-site scripting, or other types of attacks? (ARS 5.1 SI-10)	ARS 5.1 SI-10 Guidance: Ensure the system validates user input before accepting it into the system (e.g., sanitize user input within username and password fields). Note: Information input validation is relevant for systems that develop or maintain software applications or for any systems where external input is processed, whether from users, other systems, or hardware.
17.8	Does your organization ensure the information systems retains information in accordance with federal law, CMS policy, and HIPAA requirements? (ARS 5.1 SI-12)	ARS 5.1 SI-12 Guidance: Ensure that the system retains information in accordance with federal law, CMS policy, and HIPAA requirements.

18A. Program Management Controls: Attestation and Rationale

#	Question	Controls Reference
18.1	Has your organization appointed and/or identified a senior information security officer with the authority to	ARS 5.1 PM-02

	coordinate, develop, implement, and maintain an organization-wide information security program? (ARS 5.1 PM-02)	Guidance: Ensure that a Chief Information Security Officer or equivalent is appointed to manage the security program. Rationale should include the position title, description, and status of the individual appointed.

18B. Program Management Controls: Attestation

#	Question	Controls Reference
18.2	Does your organization ensure that an accurate accounting of disclosures of PII is developed and maintained to include date, nature, and purpose of each disclosure; and contact information of the person or organization to which the disclosure was made? Does your organization also ensure that the accounting of disclosures is retained for the length the PII is maintained or five years after the disclosure is made, whichever is longer, and that the accounting of disclosures is made available to the related individual upon request? (ARS 5.1 PM-21)	ARS 5.1 PM-21 Guidance: Ensure the organization keeps an accurate accounting of information disclosures in each system of records, including: a) Date, nature, and purpose of each record disclosure; and b) Contact information of the person/agency to which disclosure was made. Keep an accounting of disclosures for the life of the record or 5 years after the disclosure was made (whichever is longer). Note: Organizations should maintain a record of when and to whom PII is disclosed. This can extend to Controlled Unclassified Information, as well.

19A. Personally Identifiable Information Processing and Transparency Controls: Attestation and Rationale

Please note that there are no questions in this section. Please proceed to 19B.

19B. Personally Identifiable Information Processing and Transparency Controls: Attestation

#	Question	Controls Reference
19.1	Does your organization have a Personally Identifiable Information (PII) and Transparency policy that supports the security and privacy program and identifies the purpose, scope, roles, responsibilities, management commitment, and procedures to facilitate the implementation of the policy for the storage and processing of PII/PHI that is reviewed and updated at least every three (3) years or as needed? (ARS 5.1 PT-01)	ARS 5.1 AR-01 Guidance: Develop a Personally Identifiable Information (PII) and Transparency policy that describes: a) The purpose of the system, scope, roles, responsibilities, management commitment, coordination; and b) The procedures on how the policy is carried out. The policy and procedures should be reviewed at least every three years or as needed. Organizations may leverage overarching institutional privacy policies to satisfy this control.
19.2	Does your organization determine and document the relevant legal authority that permits the collection, use, maintenance, and sharing of PII/PHI and restrict the minimum relevant and necessary elements of PII/PHI to only that which is authorized? (ARS 5.1 PT-02)	ARS 5.1 PT-02 Guidance: Ensure that the organization determines and documents the relevant legal authority that: a) Permits the collection, use, maintenance, and sharing of PII/PHI; and b) Restricts the minimum relevant and necessary elements of PII/PHI to only that which is authorized Organizations must have clear and established authority and purpose for collecting, using, maintaining, and sharing PII/PHI.
19.3	Does your organization identify and document the purpose(s) for processing PII/PHI and restrict the	ARS 5.1 PT-03

#	Question	Controls Reference
	processing of PII/PHI to only that which is compatible with the identified purpose(s)? (ARS 5.1 PT-03)	Guidance: Ensure that the organization identifies and documents the purpose(s) for processing PII/PHI in accordance with the Data Use Agreement (DUA) and other relevant documentation.
19.4	Does your organization apply defined processing conditions or protections as required by organizational policies and determinations for specific categories of PII/PHI, where applicable? (ARS 5.1 PT-07)	ARS 5.1 PT-07 Guidance: Ensure that where applicable the organization applies special processing conditions or protections for specific categories of PII/PHI as required in organizational policies and determinations. Tailored protection should be applied to particularly sensitive types of PII/PHI. Organizations should apply special processing conditions or protections to PII/PHI categories commensurate with the level of risk if such category was subject to unauthorized disclosure or modification.

20A. Supply Chain Risk Management Controls: Attestation and Rationale
Please note that there are no questions in this section. Please proceed to 20B.

20B. Supply Chain Risk Management Controls: Attestation

#	Question	Controls Reference
20.1	Does your organization develop a policy for the implementation of supply chain risk management and a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of the systems processing, transmitting, or storing CMS data? Are the policy and plan reviewed and updated annually or as required, to address environmental changes?	ARS 5.1 SR-01, SR-02 Guidance: Develop a supply chain risk management policy and plan for managing supply chain management risks that includes all requirements. The policy and plan should be reviewed and updated at least

#	Question	Controls Reference
	(ARS 5.1 SR-01, SR-02)	every 365 days or as needed. Organization policy for supply chain risk management should focus on processes for identifying, assessing, and mitigating risks throughout the entire lifecycle of hardware, software, or IT services.
20.2	Does your organization establish a process or processes to identify and address weaknesses or deficiencies in the supply chain elements and processes of systems processing, transmitting, or storing CMS data as well as assess and review supply chain-related risks associated with suppliers or contractor services on an annual basis? (ARS 5.1 SR-03, SR-06)	ARS 5.1 SR-03, SR-06 Guidance: Ensure that the organization establishes a process or processes to identify and address weaknesses or deficiencies in the supply chain elements through assessments and reviews of supply-chain related risks associated with suppliers or contractor services. Reviews and assessments should be done on an annual basis.
20.3	Does your organization dispose of CMS data and/or system components with CMS data using techniques and methods in accordance with NIST SP 800-88 (e.g., clearing, purging, destroying, or cryptographic erasure techniques for cloud components)? (ARS 5.1 SR-12)	ARS 5.1 SR-12 Guidance: Ensure that the organization employs procedures for disposal of CMS data and/or system components with CMS data using techniques and methods in accordance with NIST SP 800-88. Disposal procedures should be employed at the end of a project or study or when CMS data is transferred to an approved computing environment.

Appendix A: Acronyms

Acronym	Explanation of acronym
AC	Access Control
ARS	Acceptable Risk Safeguards
AT	Awareness and Training
AU	Audit and Accountability
CA	Assessment, Authorization, and Monitoring
CM	Configuration Management
CMA	Computer Matching Agreement
CMS	Centers for Medicare and Medicaid Services
CP	Contingency Planning
CSP	Cloud Service Provider
CUI	Controlled Unclassified Information
DHCP	Dynamic Host Configuration Protocol
DMP SAQ	Data Management Plan Self-Attestation Questionnaire
DPSP	Data Privacy Safeguard Program
DUA	Data Use Agreement
FIPS	Federal Information Processing Standards
HIPAA	Health Insurance Portability and Accountability Act
IA	Identification and Authentication
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IR	Incident Response

Acronym	Explanation of acronym
ISA	Interconnection Security Agreement
MA	Maintenance
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MP	Media Protection
NARA	National Archives and Records Administration
NIST	National Institute of Standards of Technology
NTP	Network Time Protocol
PE	Physical and Environmental Protection
PHI	Protected Health Information
PII	Personally Identifiable Information
PL	Planning
PM	Program Management
PS	Personnel Security
PT	Personally Identifiable Information Processing and Transparency
RA	Risk Assessment
RIF	Research Identifiable File(s)
SA	System and Services Acquisition
SC	System and Communications Protection
SLA	Service-level Agreement
SI	System and Information Integrity
SIEM	Security Information and Event Management
SP	Special Publication

Acronym	Explanation of acronym
SR	Supply Chain Risk Management
USGCB	United States Government Configuration Baseline
VPN	Virtual Private Network