CMS

CENTERS FOR MEDICARE & MEDICAID SERVICES

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

September 2020

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 3.1, and
- National Institute of Standards of Technology (NIST) Special Publication (SP) 800-53 Revision 4, *Security and Privacy Controls for Federal 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 takes into account 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 the 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 3.1.

A. SECURITY 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? (ARS v3.1 AC-01)	ARS v3.1 AC-01 Guidance: Ensure an access control policy conforms to guidelines. Types of rationale may include an access control policy name and date, an outline of the policy, a paragraph explaining the policy.

#	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, and review user accounts periodically? (ARS v3.1 AC-02)	ARS v3.1 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. Types of rationale may include an outline of the account management policy that addresses the following: a) Has unique user accounts. b) Each user account has an account manager which is notified of changes. c) Has a Group/Role conditions for membership. d) Tracks 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. h) Disable emergency accounts after 24 hours. i) Disable temporary accounts within 60 days. j) Automatically disables accounts after a defined time period.

#	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 v3.1 AC-04)	ARS v3.1 AC-04 Guidance: Ensure the system controls the flow of information in accordance with approved authorizations. Types of rationale may 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 v3.1 AC-21)	ARS v3.1 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. Types of rationale may include a documented policy 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 v3.1 AC-03)	ARS v3.1 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 v3.1 AC-05)	ARS v3.1 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 audit all privileged account usage activities? (ARS v3.1 AC-06, AC-06(01), AC-06(09))	ARS v3.1 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.g. "Superuser Do" – allows users to run programs with the security privileges of another user, by default the superuser.) Audits all usage of privileged account activities.

#	Question	Controls Reference
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 v3.1 AC-07)	ARS v3.1 AC-07 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.g. “Superuser Do” – allows users to run programs with the security privileges of another user, by default the superuser.) e) Audits all usage of privileged account activities.
1.9	Does your organization’s information system display a notification or banner before granting access to the information systems? (ARS v3.1 AC-08)	ARS v3.1 AC-08 Guidance: Ensure the system displays a notification or banner before gaining access to the system which follows United States Government Configuration Baseline (USCB) guidelines. Require the user to take explicit action (e.g. clicking OK) to fully authenticate.

#	Question	Controls Reference
1.10	Does your organization's information system lock user sessions after an organization defined time limit of non-use and/or are automatically disconnected under specified circumstances? (ARS v3.1 AC-11)	ARS v3.1 AC-11 Guidance: Ensure that user sessions lock after 15 minutes, remote and internal sessions. Session lock 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).
1.11	Does your organization's information system define actions that can be taken on the system without authentication (e.g., viewing certain webpages with public information only or generic information)? (ARS v3.1 AC-14)	ARS v3.1 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).
1.12	Does your organization's remote connections have usage restrictions; have connection requirements such as cryptography connected to managed network access control points; have guidelines for user access; are monitored through audit records; and explicitly authorize the usage of privileged commands through the remote connection? (ARS v3.1 AC-17, AC-17(01), AC-17(02), AC-17(03), AC-17(04))	ARS v3.1 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.

#	Question	Controls Reference
1.13	Does your organization have usage restrictions and implementation guidance (e.g., encryption, EAP, LEAP, etc.) for wireless access and/or mobile devices? (ARS v3.1 AC-18, AC-18(01))	ARS v3.1 AC-18, AC-18(01) 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 systems outside of the its authorization boundary to store, transmit, or view system information? (ARS v3.1 AC-20, AC-20(01), AC-20(02))	ARS v3.1 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. Restrict the usage of portable storage devices (e.g. thumb drives, external hard drives) which leave the authorization boundary.
1.15	Does your organization have a process for determining what is shared with external users (e.g. collaborators)? (ARS v3.1 AC-21)	ARS v3.1 AC-21 Guidance: Ensure that the system has a process for determining what information on the system should be shared with external users

2A. Awareness and Training Controls: Attestation and Rationale

#	Question	Controls Reference
2.1	Does your organization ensure that managers, system administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems and how? (ARS v3.1 AT-02)	ARS v3.1 AT-02 Guidance: Ensure the system has a policy for completing security training. Ensure the system has a security 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 guidelines for training content. Ensure the training includes insider threat information. Types of rationale may include excerpts from the policy, training manuals, etc. that address all requirements outlined in the question.
2.2	Does your organization ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities prior to them assuming their security-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 awareness training? (ARS v3.1 AT-03)	ARS v3.1 AT-03 Guidance: Ensure the system conducts role-based training (e.g. security, incident response) within 60 days of assuming the role and every 365 days. Ensure the system maintains security and privacy awareness training and role-based system training records for 5 years after employees and contractors complete each training. Types of rationale may include excerpts from the policy, training manuals, etc. that address all requirements outlined in the question.

2B. Awareness and Training Controls

Please note that there are no questions in this control family that require an attestation. 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? (ARS v3.1 AU-01)	ARS v3.1 AU-01 Guidance: Ensure the system has a policy for audit and accountability tasks. Types of rationale may include an audit and accountability controls policy name and date, an outline of the policy, or a paragraph explaining the policy.
3.2	Does your organization have the capability to audit events on the information system 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 work stations, override of access control mechanisms, startup/shutdown of audit logging services, and audit logging service configuration changes? (ARS v3.1 AU-02)	ARS v3.1 AU-02 Guidance: Ensure the system can audit the following events: a) Server alerts and error messages b) User log-on and log-off (successful or unsuccessful) c) All system administration activities d) Modification of privileges and access e) Start up and shut down f) Application modifications g) Application alerts and error messages h) Configuration changes i) Account creation, modification, or deletion j) File creation and deletion k) Read access to sensitive information l) Modification to sensitive information m) Printing sensitive information

#	Question	Controls Reference
		n) Anomalous (e.g., non-attributable) activity o) Data as required for privacy monitoring privacy controls p) Concurrent log on from different work stations q) Override of access control mechanisms r) Process creation s) Attempts to create, read, write, modify, or delete files containing PII. Types of rationale may include excerpts from the policy, training manuals, etc. that address all requirements outlined in the question.
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., a 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 (succeed/failure); any privileged system functions executed; process creation information (command line captures if applicable)? (ARS v3.1 AU-03, AU-03(01))	ARS v3.1 AU-03, AU-03(01) Guidance: Ensure audit records contain the following metadata: a) Date and time of the event b) Component of the information system (e.g., software component, hardware component) where the event occurred c) Type of event d) User/subject identity e) Outcome (success or failure) of the event f) Program or command that initiated the event g) Execution of privileged functions h) Command line (for process creation events) i) Record disclosures of sensitive information, including protected health and financial information

#	Question	Controls Reference
		j) Log information type, date, time, receiving party, and releasing party k) Verify within every ninety (90) days for each extract that the data is erased or its use is still required. l) Filename accessed m) Source and destination IP address or hostname if applicable n) Amount of data transmitted during network session o) For systems that handle PHI, disclosures of PHI in accordance with HIPAA. Types of rationale may include excerpts from the policy, training manuals, etc. that 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 for 90 days of audit records? (ARS v3.1 AU-04, AU-11)	ARS v3.1 AU-04, AU-11 Guidance: Ensure adequate storage capacity for 90 days of audit records. Shut down the system if audit records run out of storage.
3.5	Does your organization ensure that administrators are notified of process failures through the audit process of the information systems? (ARS v3.1 AU-05)	ARS v3.1 AU-05 Guidance: Ensure there is a standard operating procedure for handling audit system processing failures or instances where audit storage capacity is exceeded without disabling auditing.

#	Question	Controls Reference
3.6	Does your organization ensure that: Audit records are reviewed weekly and manually every 30 days; 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 v3.1 AU-06, AU-06(03))	ARS v3.1 AU-06, AU-06(03) Guidance: Ensure audit records are reviewed weekly. Manually review audit records every 30 days. 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 v3.1 AU-07(01), AU-07(02))	ARS v3.1 AU-07(01), AU-07(02) Guidance: Audit records shall be searchable.
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 v3.1 AU-08, AU-08(01))	ARS v3.1 AU-08, AU-08(01) Guidance: Ensure internal system clocks are regularly synchronized with NIST time servers and that audit records user internal system clocks to generate a time stamp.
3.9	Does your organization ensure the audit records and tools are protected from unauthorized access, deletion and modification? Is access to these audit records limited to a subset of privileged users? (ARS v3.1 AU-09, AU-09(04))	ARS v3.1 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 (1) year in archive storage? (ARS v3.1 AU-11)	ARS v3.1 AU-11 Guidance: Retain audit records for 90 days in “hot” storage and archive storage for 1 year. Comply with NARA requirements for storage.

4A. Security Assessment and Authorization Controls: Attestation and Rationale

#	Question	Controls Reference
4.1	Does your organization have a policy for security assessment and authorization activities? (ARS v3.1 CA-01)	ARS v3.1 CA-01 Guidance: Ensure the system has a policy for assessment and authorization policies. Types of rationale may include a security assessment and authorization controls policy name and date, an outline of the policy, or a paragraph explaining the policy.
4.2	Does your organization ensure that any external and internal interconnections, if applicable, have documented authorization decisions for connections from the system to other systems using some form of agreement (MOU, MOA, ISA, etc.); document the interface, security requirements, and type of information exchanged; and establish timeframes for reviewing and updating ISAs? (ARS v3.1 CA-03, CA-03(05), CA-09)	ARS v3.1 CA-03, CA-03(05), CA-09 Guidance: Ensure that external and internal interconnections have: a) An Interconnection Security Agreement (or MOU or MOA) b) Documented interface, security requirements, and type of information exchanged c) Updated ISAs once per year or after a significant change *ISAs are not necessary if the same IT infrastructure management is used. Types of rationale may include excerpts from the policy, training manuals, etc. that address all requirements outlined in the question.

#	Question	Controls Reference
4.3	Does your organization use a deny-all, permit-by-exception policy for system access to ensure that only those connections which are essential and approved are allowed? (ARS v3.1 CA-03(05))	ARS v3.1 CA-03(05) Guidance: Ensure the system uses a deny-all, permit-by-exception policy for system access. Types of rationale may include excerpts from the policy, training manuals, etc. that address all requirements outlined in the question.

4B. Security Assessment and Authorization Controls: Attestation

#	Question	Controls Reference
4.4	Does your organization have a continuous monitoring program that manages identified vulnerabilities, remediation and ongoing security assessments? (ARS v3.1 CA-07)	ARS v3.1 CA-07 Guidance: Ensure the system has a continuous monitoring program which monitors: a) Metrics related to identified vulnerabilities and remediation. b) Ongoing security assessments (DMP process counts as a security assessment).

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? (ARS v3.1 CM-01)	ARS v3.1 CM-01 Guidance: Ensure the system has a policy for configuration management. Types of rationale may include a configuration management controls policy name and date, an outline of the policy, or a paragraph explaining the policy.
5.2	Does your organization track, review, approve or disapprove, and log changes to organizational information systems? (ARS v3.1 CM-03)	ARS v3.1 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 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 on the production system Types of rationale may include excerpts from the policy, training manuals, etc. that address all requirements outlined in the question.

#	Question	Controls Reference
5.3	Does your organization establish and enforce security configuration settings for information technology products employed in the organizational information systems? (ARS v3.1 CM-06)	ARS v3.1 CM-06 Guidance: Ensure the system: a) Documents default configuration settings which follow the most restrictive mode possible for reliable operation b) Implements the configuration settings c) Documents any configuration deviations d) Monitors configuration changes e) Follow United States Government Configuration Baselines or similar configuration standards. Types of rationale may include excerpts from the policy, training manuals, etc. that 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 hosts within the information system? (ARS v3.1 CM-02)	ARS v3.1 CM-02 Guidance: Ensure the system has a current baseline configuration image for hosts 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 which constitute a significant change, the baseline configuration shall be updated.

#	Question	Controls Reference
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 v3.1 CM-05)	ARS v3.1 CM-05 Guidance: Ensure the system uses physical and logical access restrictions to prevent unauthorized changes to the system.
5.6	Does your organization ensure that configuration of the information systems allows only essential functions, software, ports, protocols, and applications? (ARS v3.1 CM-07)	ARS v3.1 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.

#	Question	Controls Reference
5.7	Does your organization maintain 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 v3.1 CM-08, CM-08(01))	ARS v3.1 CM-08, CM-08(01) Guidance: Ensure the system maintains an up-to-date system inventory which includes all components within the boundary. Metadata shall include: a) Each component's unique identifier and/or serial number b) Information system of which the component is a part c) Type of information system component (e.g., server, desktop, application) d) Manufacturer/model information e) Operating system type and version/service pack level f) Presence of virtual machines g) Application software version/license information h) Physical location (e.g., building/room number) i) Logical location (e.g., IP address, position with the information system [IS] architecture) j) Media access control (MAC) address k) Ownership l) Operational status m) Primary and secondary administrators n) Primary use
5.8	Does your organization ensure that the information system prevents users from installing non-approved software through user policies? (ARS v3.1 CM-11)	ARS v3.1 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? (ARS v3.1 CP-01)	ARS v3.1 CP-01 Guidance: Ensure the system has a policy for contingency planning. Types of rationale may include a contingency planning policy name and date, an outline of the policy, a paragraph explaining the policy.
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-related documentation backups? How does your organization protect the confidentiality, integrity, and availability of backup information at the storage locations? (ARS v3.1 CP-09)	ARS v3.1 CP-09 Guidance: Ensure the system performs full weekly and incremental daily backups of: a) User level data b) System data c) System documentation Backup archives shall include 3 full backups and be stored offsite. Types of rationale may include excerpts from the policy, training manuals, etc. that address all requirements outlined in the question.

6B. Contingency Planning Controls: Attestation

Please note that there are no questions in this control family that require an attestation. 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? (ARS v3.1 IA-01)	ARS v3.1 IA-01 Guidance: Ensure the system has an Identification and Authentication policy. Types of rationale may include an identification and authentication policy name and date, an outline of the policy, a paragraph explaining the policy.
7.2	Does your organization authenticate the identities of users, processes, or devices prior to granting access to organizational systems? 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 v3.1 IA-02, IA-03, IA-05)	ARS v3.1 IA-02, IA-03, IA-05 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) Prohibits the use of dictionary names or words d) Meets or exceeds enforcement of the following minimum password requirements: 1. MinimumPasswordAge = one (1) day 2. MaximumPasswordAge = sixty (60) days 3. MinimumPasswordLength = Minimum length of eight (8) characters for regular user passwords, and minimum length of fifteen (15) characters for administrators or privileged user passwords 4. PasswordComplexity = minimum (three (3) for

#	Question	Controls Reference
		High or one (1) for Moderate or Low) character(s) from the four (4) character categories (A-Z, a-z, 0-9, special characters 5. PasswordHistorySize = twelve (12) passwords for High or six (6) passwords for Moderate or Low systems. e) The minimum length (MinimumPasswordLength) for administrators or privileged users is fifteen (15) characters f) If the operating environment enforces a minimum of number of changed characters when new passwords are created, set the value at twelve (12) for High and six (6) for Moderate or Low systems; g) Stores and transmits only encrypted representations of passwords; and h) 8. Allows the use of a temporary password for system logons with an immediate change to a permanent password Types of rationale may include excerpts from the policy, training manuals, etc. that 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 v3.1 IA-02)	ARS v3.1 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 v3.1 IA-03)	ARS v3.1 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 (3) years; and disable identifiers after 60 days of inactivity? (ARS v3.1 IA-04	ARS v3.1 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 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 v3.1 IA-06)	ARS v3.1 IA-06 Guidance: Ensure the system shows non-descript information when authentication fails.

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? (ARS v3.1 IR-01)	ARS v3.1 IR-01 Guidance: Ensure the system has an incident response policy. Types of rationale may include an incident response policy name and date, an outline of the policy, a paragraph explaining the policy.
8.2	How does your organization investigate (e.g., preparation, detection, analysis, containment, eradication, and recovery) and track security incidents (e.g. physical, technical, and privacy)? (ARS v3.1 IR-04, IR-05)	ARS v3.1 IR-04, IR-05 Guidance: Ensure the system 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 personnel to report potential incidents and investigate the potential incident. Types of rationale may include excerpts from the policy, training manuals, etc. that address all requirements outlined in the question.

8B. Incident Response Controls: Attestation

#	Question	Controls Reference
8.3	Does your organization ensure that employees whom have incident response duties complete incident response training within one (1) month of assuming the role and complete/update incident response training at least once a year? (ARS v3.1 IR-02)	ARS v3.1 IR-02 Guidance: Ensure that employees which have incident response duties complete incident response training with 1 month of assuming the role and every 365 days. Conduct incident response training every 365 days.

#	Question	Controls Reference
8.4	Does your organization have the capability to investigate security incidents, that includes preparation, detection, analysis, containment, eradication, and recovery? (ARS v3.1 IR-04, IR-05)	ARS v3.1 IR-04, IR-05 Guidance: Ensure the system can investigate security incidents, to include preparation, detection, analysis, containment, eradication, and recovery.
8.5	Does your organization investigate (e.g., preparation, detection, analysis, containment, eradication, and recovery) and track security incidents (e.g., physical, technical, and privacy)? (ARS v3.1 IR-04, IR-05)	ARS v3.1 IR-04, IR-05 Guidance: Ensure the system 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).
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.)? (ARS v3.1 IR-07)	ARS v3.1 IR-07 Guidance: Ensure the system has an incident response resource which can assist system administrators.
8.7	Does your organization's information system 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; reviewed and approved by the applicable Incident Response Team Leader; distributes copies of the incident response plan to the organization's information security officers and other incident response team personnel; review the incident response plan within every 365 days; update the incident response plan to address system/organizational changes or problems encountered during plan implementation,	ARS v3.1 IR-08 Guidance: Ensure the system has an incident response plan which: a) Provides the organization with a roadmap for implementing its incident response capability b) Describes the structure and organization of the incident response capability c) Provides a high-level approach for how the incident response capability fits into the overall organization d) Meets the unique requirements of the organization, which relate to mission, size, structure, and functions e) Defines reportable incidents

#	Question	Controls Reference
	execution, or testing; communicate incident response plan changes to the organizational elements listed above; and protects the incident response plan from unauthorized disclosure and modification? (ARS v3.1 IR-08)	f) Provides metrics for measuring the incident response capability within the organization g) Defines the resources and management support needed to effectively maintain and mature an incident response capability h) Is reviewed and approved by the applicable Incident Response Team Leader i) Distributes copies of the incident response plan to: 1. CMS Chief Information Security Officer 2. CMS Chief Information Officer 3. Information System Security Officer 4. CMS Office of the Inspector General/Computer Crimes Unit 5. All personnel within the organization Incident Response Team 6. All personnel within the PII Breach Response Team 7. All personnel within the organization Operations Centers j) Reviews the incident response plan within every three hundred sixty-five (365) days k) Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing l) Communicates incident response plan changes to the

#	Question	Controls Reference
		organizational elements listed above m) Protects the incident response plan from unauthorized disclosure and modification.

9A. Maintenance Controls: Attestation and Rationale

Please note that there are no questions in this control family that require an attestation with rationale. 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? (ARS v3.1 MA-01)	ARS v3.1 MA-01 Guidance: Develop a System Maintenance Policy and distribute it to the applicable personnel. It should describe: a) The purpose of the system, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. b) The procedures on how the policy is carried out. The policy and procedures are reviewed at least every three (3) years or sooner if there is a major change to the system.
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 v3.1 MA-03, MA-03(01))	ARS v3.1 MA-03, MA-03(01) Guidance: Ensure the system utilizes diagnostic hardware, software, or firmware maintenance tools within the data center that have not been improperly modified.

9.3	Does your organization check media containing diagnostic and test programs being introduced into the system for malicious code, where applicable? (ARS v3.1 MA-03(02))	ARS v3.1 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

Please note that there are no questions in this control family that require an attestation with rationale. Please proceed to 10b.

10B. Media Protection Controls: Attestation

#	Question	Controls Reference
10.1	Does your organization have a media protection policy that is reviewed/updated at least once a year? (ARS v3.1 MP-01)	ARS v3.1 MP-01 Guidance: Develop a Media Protection Policy and distribute it to the applicable personnel. The policy should describe: a) The purpose of the system, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. b) The procedures of how the policy is carried out. The policy and procedures are reviewed at least every three (3) years or sooner if there is a major change to the system.
10.2	Does your organization ensure the information system administrators mark system media based on the classification of information the media holds? (ARS v3.1 MP-03)	ARS v3.1 MP-03 Guidance: Ensure the system marks system media based on the classification of information the media holds.
10.3	Does your organization protect and securely stores digital media and ensure it is overwritten once with a "00000000x"	ARS v3.1 MP-04, MP-06

#	Question	Controls Reference
	pattern or degaussed with a NIST approved degaussing device? (ARS v3.1 MP-04, MP-06)	Guidance: Ensure the system securely stores digital media and is overwritten once with a "00000000x" pattern or degaussed with a NIST approved magnet.
10.4	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 v3.1 MP-05)	ARS v3.1 MP-05 Guidance: Ensure the system protects 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.
10.5	Does your organization sanitize media prior to disposal or reuse and track such activities? (ARS v3.1 MP-06, MP-06(01))	ARS v3.1 MP-06, MP-06(01) Guidance: Ensure the system sanitizes media prior to disposal or reuse and tracks such activities.
10.6	Does your organization prohibit the use of personally owned media? (ARS v3.1 MP-07, MP-07(01))	ARS v3.1 MP-07, MP-07(01) Guidance: Ensure the system prohibits the use of personally owned media.
10.7	Does your organization ensure that any portable media devices have an identified owner? (ARS v3.1 MP-07, MP-07(01))	ARS v3.1 MP-07, MP-07(01)

#	Question	Controls Reference
		Guidance: Ensure any portable media devices have an identified owner.
10.8	Does your organization ensure that records of disposed media which contain sensitive information are maintained? (ARS v3.1 MP-CMS-01)	ARS v3.1 MP-CMS-01 Guidance: Ensure that records of disposed media which contain sensitive information are maintained.

11A. Physical and Environmental Controls: Attestation and Rationale

Please note that there are no questions in this control family that require an attestation with rationale. 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? (ARS v3.1 PE-01)	ARS v3.1 PE-01 Guidance: Develop a Physical and Environmental Protection Policy and distribute it to the applicable personnel. The policy should describe: a) The scope, roles and responsibilities of the system. b) The Procedures to carry out the implementation of the Physical and Environmental Protection Policy. Review and update the current policy and procedures every three (3) years or in case of a major change in the system.

#	Question	Controls Reference
11.2	Does your organization maintain a current list of authorized individuals to enter the facility? (ARS v3.1 PE-02)	ARS v3.1 PE-02 Guidance: Ensure the system maintains a current list of authorized individuals to enter the facility.
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 v3.1 PE-03)	ARS v3.1 PE-03 Guidance: Ensure the system: a) Verifying individual access authorizations before granting access to the facility b) Controlling ingress/egress to the facility using guards and/or defined physical access control systems/devices (defined in the applicable security plan) c) Maintains physical access audit logs for defined entry/exit points (defined in the applicable security plan) d) Provides defined security safeguards (defined in the applicable security plan) to control access to areas within the facility officially designated as publicly accessible e) Escorts visitors and monitors visitor activity in defined circumstances requiring visitor escorts and monitoring (defined in the applicable security plan) f) Secures keys, combinations, and other physical access devices g) Inventories defined physical access devices (defined in the applicable security plan) no less often than every (90 High, 90 Moderate, or 180 Low) days

#	Question	Controls Reference
		h) Changes combinations and keys for defined high-risk entry/exit points (defined in the applicable security plan) within every 365 days, and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.
11.4	Does your organization ensure that telephone and network hardware and transmission lines are protected? (ARS v3.1 PE-04)	ARS v3.1 PE-04 Guidance: Ensure that telephone and network hardware and transmission lines are protected.
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 v3.1 PE-04)	ARS v3.1 PE-04 Guidance: Ensure that all physical ports (e.g., wiring closets, patch panels, etc.) are disabled.

12A. Planning Controls: Attestation and Rationale

#	Question	Controls Reference
12.1	Does your organization have a complete and up-to-date system security plan? How often is it reviewed/updated? (ARS v3.1 PL-02)	ARS v3.1 PL-02 Guidance: Ensure the system has a completed and up-to-date system security plan which includes the required information. Types of rationale may include a system security plan name and date, an outline of the plan, or a paragraph explaining the plan.

#	Question	Controls Reference
12.2	Does your organization ensure that rules of behavior (e.g. user agreements, system use agreements, etc.) are signed by all users and administrators? Is this updated/reviewed at least once a year? How is it acknowledged? (ARS v3.1 PL-04)	ARS v3.1 PL-04 Guidance: Ensure that rules of behavior are signed by all users. Types of rationale may include excerpts from the policy, training manuals, etc. that address all requirements outlined in the question.

12B. Planning Controls: Attestation

Please note that there are no questions in this control family that require an attestation. Please proceed to 13b.

13A. Personnel Security Controls: Attestation and Rationale

Please note that there are no questions in this control family that require an attestation with rationale. Please proceed to 13b.

13B. Personnel Security Controls: Attestation

#	Question	Controls Reference
13.1	Does your organization follow CMS policy regarding background checks and screening for employees with access to CMS data? (ARS v3.1 PS-03)	ARS v3.1 PS-03 Guidance: Ensure the system follows CMS policy in regard to background checks and screening for employees with access to CMS data.
13.2	Does your organization ensure that employee termination follows the following steps: Disables information system access before or during termination; terminates/revokes any authenticators/credentials associated with the individual; conducts exit interviews that include a discussion of non-disclosure of information security and privacy information; retrieves all security-related organizational information system-related property; retains access to organizational	ARS v3.1 PS-04 Guidance: Ensure that employee termination follows the following steps: a) Disables information system access before or during termination; b) Terminates/revokes any authenticators/credentials

#	Question	Controls Reference
	information and information systems formerly controlled by the terminated individual; notifies defined personnel or roles (defined in the applicable security plan) within one (1) calendar day; and immediately escorts employees terminated for cause out of the organization? (ARS v3.1 PS-04)	associated with the individual; c) Conducts exit interviews that include a discussion of non-disclosure of information security and privacy information; d) Retrieves all security-related organizational information system-related property; e) Retains access to organizational information and information systems formerly controlled by the terminated individual; f) Notifies defined personnel or roles (defined in the applicable security plan) within one (1) calendar day; and g) Immediately escorts employees terminated for cause out of the organization.
13.3	Does your organization have processes for re-screening personnel according to organizationally defined conditions as required? (ARS v3.1 PS-03)	ARS v3.1 PS-03 Guidance: Ensure that the organization established procedures for re-screening personnel consistent with criticality/ sensitivity risk designation of the position and based on organizational policy.
13.4	Does your organization ensure that users sign access agreements every 365 days? (ARS v3.1 PS-06)	ARS v3.1 PS-06 Guidance: Ensure that users sign access agreements every 365 days.

#	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 v3.1 PS-07)	ARS v3.1 PS-07 Guidance: Ensure that 3rd party service providers (contractors, CSPs, vendor maintenance) follow the same personnel requirements as full-time employees.
13.6	Does your organization ensure that the organization has a formal sanction process for employees who violate security policies or procedures? (ARS v3.1 PS-08)	ARS v3.1 PS-08 Guidance: Ensure the system has a formal sanction process for employees which violate security policies or procedures.

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 v3.1 RA-05)	ARS v3.1 RA-05 Guidance: Ensure the system utilizes an automated vulnerability scanner which complies with organizational policies. Scans should be ran once every 72 hours or when a new threat has been discovered. Remediation shall also comply with DHS policies. Scans must be authenticated to the target system as a privileged user. Types of rationale may include excerpts from the policy, training manuals, etc. that address all requirements outlined in the question.

14B. Risk Assessment Controls: Attestation

Please note that there are no questions in this control family that require an attestation. Please proceed to 15b.

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

Please note that there are no questions in this control family that require an attestation with rationale. Please proceed to 15b.

15B. System and Services Acquisition Controls: Attestation

#	Question	Controls Reference
15.1	Does your organization's administrators: Document configuration of the individual hosts within the system; how to perform maintenance of security functions; known vulnerabilities (can be tracked through a Plan of Action and Milestones (POA&M)); and other documentation as needed for use and operation of the system? (ARS v3.1 SA-05)	ARS v3.1 SA-05 Guidance: Ensure the system is well documented by the administrators, to include: a) Configuration of the individual hosts within the system b) How to perform maintenance of security functions c) Known vulnerabilities (can be tracked through a POA&M) d) Other documentation as needed for use and operation of the system.
15.2	Does your organization ensure that the information system architecture is designed following security engineering principles (consistent with NIST SP 800-160 Volume 1)? (ARS v3.1 SA-08)	ARS v3.1 SA-08 Guidance: Ensure that the system architecture is designed following security engineering principles.
15.3	Does your organization ensure that any external services (third-party tools for ticketing, messaging, auditing, monitoring, etc.) outside of the accreditation/authorization boundary comply with organizational information security requirements? (ARS v3.1 SA-09)	ARS v3.1 SA-09 Guidance: Ensure that providers of any external information system services comply with organizational information security requirements and employ appropriate security and privacy controls.

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 boundaries and key internal boundaries of organizational systems? What type of system is used? (ARS v3.1 SC-07)	ARS v3.1 SC-07 Guidance: Ensure the system has boundary protection (e.g. firewall, IDS/IPS): 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 d) 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 AU e) Logs from devices must be sent to the organizations SIEM as defined within AU Types of rationale may include excerpts from the policy, training manuals, etc. that address all requirements outlined in the question.

#	Question	Controls Reference
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 v3.1 SC-08, SC-13, SC-28)	FIPS 140-2, ARS v3.1 SC-08, SC-13, SC-28 Guidance: Ensure the system uses FIPS 140-2 validated cryptographic modules for transmission of data. Ensure the system uses FIPS 140-2 validated cryptographic modules for protecting data at rest. Types of rationale may include excerpts from the policy, training manuals, etc. that address all requirements outlined in the question.

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 v3.1 SC-02)	ARS v3.1 SC-02 Guidance: Ensure that administrative and regular user interfaces are separate.
16.4	Does your organization ensure the information system has the ability to terminate a network connection at the end of the session or after a defined period of inactivity? (ARS v3.1 SC-10)	ARS v3.1 SC-10 Guidance: Ensure that the system can terminate a network connection at the end of session or automatically disconnects after a defined period activity. Examples include, but are not limited to, Dynamic Host Configuration Protocol (DHCP) sessions or VPN connection.

#	Question	Controls Reference
16.5	Does your organization have a centralized cryptographic key management system that complies with organizational standards? (ARS v3.1 SC-12)	ARS v3.1 SC-12 Guidance: Ensure the system has a cryptographic key management system which complies with HHS standards.
16.6	Does your organization prohibit collaborative computing mechanisms (e.g. networked white boards, cameras, microphones, etc.) unless explicitly authorized? (ARS v3.1 SC-15)	ARS v3.1 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 and provides an indication of use to those users present at the device.

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 v3.1 SI-03)	ARS v3.1 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 Types of rationale may include excerpts from the policy, training manuals, etc. that address all requirements outlined in the question.

#	Question	Controls Reference
17.2	How 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 v3.1 SI-04, SI-04(04))	ARS v3.1 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. Types of rationale may include excerpts from the policy, training manuals, etc. that address all requirements outlined in the question.
17.3	Does your organization use file integrity monitoring (FIM), deploy 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 v3.1 SI-07)	ARS v3.1 SI-07 Guidance: Ensure the system uses file integrity monitoring to monitor changes to the system. Types of rationale may include excerpts from the policy, training manuals, etc. that address all requirements outlined in the question.

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 ten (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 v3.1 SI-02)	ARS v3.1 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.
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 v3.1 SI-03)	ARS v3.1 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
17.6	Are email servers being hosted by the organization in the authorization boundary? Are spam filters used with the mail servers? (ARS v3.1 SI-08)	ARS v3.1 SI-08 Guidance: If the system has an e-mail server, ensure that spam protection is used.
17.7	Does your organization's information system validate user input before accepting it into the system (e.g., sanitize user input within username and password fields)? (ARS v3.1 SI-10)	ARS v3.1 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).

#	Question	Controls Reference
17.8	Does your organization ensure the information systems retains information in accordance with federal law, CMS policy, and HIPAA requirements? (ARS v3.1 SI-12)	ARS v3.1 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 coordinate, develop, implement, and maintain an organization-wide information security program? (ARS v3.1 PM-02)	ARS v3.1 PM-02 Guidance: Ensure that a Chief Information Security Officer is appointed to manage the security program. Types of rationale may include the position title, description, and status of the individual appointed.

18B. Program Management Controls: Attestation

Please note that there are no questions in this control family that require an attestation. Please proceed to the Privacy Controls.

B. PRIVACY CONTROLS

19. Accountability, Audit and Risk Management: Attestation

#	Question	Controls Reference
19.1	Does your organization have an office or department responsible for overseeing data privacy, the monitoring of privacy laws and policies, and the development of a strategic organizational privacy plan? (ARS v3.1 AR-01)	ARS v3.1 AR-01 Guidance: Ensure the following: a) Appoint a Senior Agency Official for Privacy (SAOP) or Chief Privacy Officer. b) Monitor privacy laws and policy affecting the organization's privacy program. c) Allocate sufficient budget/resources to implement and operate the organization's privacy program. d) Develop a strategic organizational privacy plan for implementing applicable privacy controls, policies, and procedures. e) Develop, disseminate, and implement operational privacy policies and procedures on privacy controls for PII-related programs, information systems or technologies. f) Update privacy plan, policies, and procedures at least every 2 years.

#	Question	Controls Reference
19.2	Does your organization review a random sample of contracts for contractors and service providers every two (2) years that provides maintenance for a system of records; ensures that the contracts include Privacy Act compliance clauses; and has defined privacy roles, responsibilities, and access requirements? (ARS v3.1 AR-03)	ARS v3.1 AR-03 Guidance: Ensure defined privacy roles, responsibilities, and access requirements for contractors and service providers. Every 2 years, the organization reviews a random sample of contracts that provide maintenance of a systems of records ensuring that the contracts include Privacy Act compliance clauses.
19.3	Does your organization monitor privacy policies and audit privacy controls at least once every year? (ARS v3.1 AR-04)	ARS v3.1 AR-04 Guidance: Ensure organization monitors and audits privacy controls and privacy policy at least once every 365 days.
19.4	Does your organization develop, implement, and routinely update a comprehensive privacy training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures? (ARS v3.1 AR-05a)	ARS v3.1 AR-05a Guidance: Ensure the organization: a) Develops, implements, and updates a comprehensive privacy training and awareness strategy; b) Administers basic training as well as role-based privacy training at least once every 365 days. c) Ensure that personnel certify (manually/electronically) acceptance of responsibilities for privacy requirements no less than once every 365 days.

#	Question	Controls Reference
19.5	Does your organization ensure that personnel (manually or electronically) accept responsibilities for privacy requirements, including their obligation to protect the confidentiality and integrity of data, at least once every year? (ARS v3.1 AR-05b, c)	ARS v3.1 AR-05b, c Guidance: Ensure the organization: a) Develops, implements, and updates a comprehensive privacy training and awareness strategy; b) Administers basic training as well as role-based privacy training at least once every 365 days. c) c) Ensure that personnel certify (manually/electronically) acceptance of responsibilities for privacy requirements no less than once every 365 days.
19.6	Does your organization ensure that an accurate accounting of information disclosures is in each system of records to include: the date, nature, purpose of each record disclosure, and list the address of a person or agency to whom the disclosure was made, for the life of the record or five (5) years after the disclosure was made (whichever is longer), and available to the person named in record upon request? (ARS v3.1 AR-08)	ARS v3.1 AR-08 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; b) Name and address of a 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). Makes accounting of disclosure available to person named in record upon request.

#	Question	Controls Reference
19.7	Does your organization have an accountability, audit, and risk management policy that 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 two (2) years or as needed? (ARS v3.1 AR-CMS-01)	ARS v3.1 AR-CMS-01 Guidance: Develop an Accountability, Audit, and Risk Management Policy and distribute it to the applicable personnel. The policy should describe: a) The purpose, scope, roles, responsibilities, management, commitment, coordination among organizational entities, and compliance; and b) Procedures to help implement the policy and associated controls. Review and update the current policy and procedures every 2 years or when there has been a significant change in privacy laws, regulation and policy affecting the internal privacy policy as needed.

20. Authority and Purpose: Attestation

#	Question	Controls Reference
20.1	Does your organization have an authority and purpose policy that 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 two (2) years or as needed? (ARS v3.1 AP-CMS-01)	ARS v3.1 AP-CMS-01 Guidance: Develop an Authority and Purpose policy and disseminates to applicable personnel. The policy should address: a) The purpose, scope, roles, responsibilities, management commitment b) Procedures to facilitate the implementation of an Authority and Purpose policy associated with related controls. The organization reviews and updates the current policy and procedures at least every 2 years as needed.

21. Data Minimization and Retention: Attestation

#	Question	Controls Reference
21.1	Does your organization ensure that the minimum personally identifiable information (PII) elements identified are relevant and necessary to accomplish collection and have express CMS authorization? (ARS v3.1 DM-CMS-01)	ARS v3.1 DM-CMS-01 Guidance: Identify minimum PII elements that are relevant and necessary to accomplish collection (and where the collection of certain PII requires legal authorization).* Limit the collection and retention of PII to the minimum elements identified in the notice and (when the collection of PII is made from the subject individual) limit its purposes to those for which the individual provided consent to (as permitted by the law). Conduct an initial evaluation of PII holdings and establish/follow a schedule for a regular review of those holdings at least once every 365 days. Ensure that only PII identified in notices is collected and retained and PII continues to be necessary to accomplish legally authorized purpose. *HHS/CMS must ensure PII is legally authorized

22. Data Quality and Integrity: Attestation

#	Question	Controls Reference
22.1	Does your organization have a data quality and integrity policy that 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 two (2) years or as needed? (ARS v3.1 DI-CMS-01)	ARS v3.1 DI-CMS-01 Guidance: The organization develops and documents to disseminate to applicable personnel the following: a) A Data Quality and Integrity Policy that outlines the purpose, scope, roles, responsibilities, management commitment, coordination (among organizational entities), and compliance. b) Procedures to make implementation of Data Quality and Integrity Policy and associated controls easier. The organization reviews and updates the current Data Quality and Integrity Policy and Procedures within every 2 years as needed.

23. Individual Participation and Redress: Attestation

#	Question	Controls Reference
23.1	Does your organization have an individual participation and redress policy that 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 two (2) years or as needed? (ARS v3.1 IP-CMS-01)	ARS v3.1 IP-CMS-01 Guidance: Develop, document, and disseminate: a) An Individual Participation and Redress Policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. b) Procedures to help implement the Individual Participation Redress Policy and related controls. Review and update the current Individual Participation and Redress Policy and procedures at least every 2 years as needed.

24. Security: Attestation

#	Question	Controls Reference
24.1	Does your organization have a security policy that 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 two (2) years or as needed? (ARS v3.1 SE-CMS-01)	ARS v3.1 SE-CMS-01 Guidance: Develop, document, and disseminate: a) A security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination, and compliance to applicable personnel. b) Procedures to help implement security policy and controls. Review and update the current security policy and procedures at least every 2 years as needed.

25. **Transparency:** Attestation

#	Question	Controls Reference
25.1	Does your organization have a transparency policy that 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 two (2) years or as needed? (ARS v3.1 TR-CMS-01)	ARS v3.1 TR-CMS-01 Guidance: Develop, documents, and disseminate: a) A Transparency Policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities and compliance; and b) Procedures help implement the Transparency Policy and related controls. Review and update the current policy and procedures at least every 2 years as needed.

26. **Use Limitation:** Attestation

#	Question	Controls Reference
26.1	Does your organization have a use limitation policy that 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 two (2) years or as needed? (ARS v3.1 UL-CMS-01)	ARS v3.1 UL-CMS-01 Guidance: Develop, documents, and disseminates: a) The Use Limitation Policy that addresses, purpose, scope, roles, responsibilities, management commitment, coordination among organization entities, and compliance. b) Procedures to help the implementation of the Use Limitation Policy and associated controls. Review and update the current use limitation policy and

#	Question	Controls Reference
		procedures at least every 2 years as necessary.
26.2	Does your organization use PII or PHI internally – only for authorized purpose(s) identified in the Privacy Act, and externally – only for authorized purposes by permission of an authorized business associate agreement with third parties, specifically describing the PII and the purpose for which it may be used? (ARS v3.1 UL-01, UL-02a, b)	ARS v3.1 UL-01, UL-02a, b Guidance: Use PII (or PHI) internally only for authorized purpose(s) identified in the Privacy Act and/or in public notices in systems that process, tore, or transmit PII/PHI. "Use PII (or PHI) internally only for authorized purpose(s) identified in the Privacy Act and/or in public notices in systems that process, tore, or transmit PII/PHI. Enter into MOUs, MOAs, Letters of Intent, CMAs or similar agreements with 3rd parties specifically describing PII covered and describing purposes for which PII may be used. Monitor, audit, and train staff on authorized sharing of PII with 3rd parties to assess whether the sharing is authorized, and an additional/new public notice is required."

#	Question	Controls Reference
26.3	Does your organization monitor, audit, and train its staff on the authorized sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII as well as evaluate any proposed new instances of sharing PII with third parties? (ARS v3.1 UL-02c, d)	ARS v3.1 UL-02c, d Guidance: "Use PII (or PHI) internally only for authorized purpose(s) identified in the Privacy Act and/or in public notices in systems that process, tore, or transmit PII/PHI. Enter into MOUs, MOAs, Letters of Intent, CMAs or similar agreements with 3rd parties specifically describing PII covered and describing purposes for which PII may be used. Monitor, audit, and train staff on authorized sharing of PII with 3rd parties to assess whether the sharing is authorized, and an additional/new public notice is required."

Appendix A: Acronyms

Acronym	Explanation of acronym
AC	Access Control
AP	Authority and Purpose
AR	Accountability, Audit, and Risk Management
ARS	Acceptable Risk Safeguards
AT	Awareness and Training
AU	Audit and Accountability
CA	Security Assessment and Authorization
CM	Configuration Management
CMA	Computer Matching Agreement
CMS	Centers for Medicare and Medicaid Services
CP	Contingency Planning
DHCP	Dynamic Host Configuration Protocol
DUA	Data Use Agreement(s)
DI	Data Quality and Integrity
DM	Data Minimization and Retention
DMP SAQ	Data Management Plan Self-Attestation Questionnaire
DPSP	Data Privacy Safeguard Program
FIPS	Federal Information Processing Standards
HHS	Department of Health and Human Services
IA	Identification and Authentication
IP	Individual Participation and Redress

Acronym	Explanation of acronym
IR	Incident Response
MA	Maintenance
MP	Media Protection
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NIST	National Institute of Standards of Technology
PE	Physical and Environmental Protection
PL	Planning
PM	Program Management
PS	Personnel Security
RA	Risk Assessment
RIF	Research Identifiable File(s)
SA	System and Services Acquisition
SC	System and Communications Protection
SE	Security
SI	System and Information Integrity
TR	Transparency
USCB	United States Government Configuration Baseline
US CERT	United States Computer Emergency Readiness Team
UL	Use Limitation