DATA PRIVACY SAFEGUARD PROGRAM
DATA MANAGEMENT PLAN SELF-ATTESTATION QUESTIONNAIRE (DMP SAQ)

PURPOSE: The CMS data your organization is requesting contains sensitive information that requires evidence that adequate data security and privacy safeguards are in place to protect the confidentiality, integrity, and availability of CMS data. The following questionnaire will support your organization in attesting and demonstrating your compliance with CMS safeguard requirements, specifically the CMS Acceptable Risk Safeguards (ARS) 3.1 Publication.

1. DUA ORGANIZATION INFORMATION

REQUESTING ORGANIZATION	Click here to enter text.
COMPUTING ENVIRONMENT NAME	Click here to enter text.
COMPUTING ENVIRONMENT TYPE	☐ Cloud Service Provider (CSP) ☐ Onsite ☐ Hybrid: Uses CSP & Exists Onsite
COMPUTING ENVIRONMENT ADDRESS	Click here to enter text.

2. DATA CUSTODIAN

The Data Custodian is the individual who will be responsible for the observance of all the conditions of use for the environment identified in this document, including the establishment and maintenance of security arrangements to prevent unauthorized use. The Data Custodian must sign the DMP SAQ (in section 6) prior to submission. Please note that the DMP SAQ only allows for a single Data Custodian. Additional Data Custodians may be added to individual DUAs, if necessary.

DATA CUSTODIAN	Click here to enter text.
DATA CUSTODIAN OFFICE ADDRESS	Click here to enter text.
DATA CUSTODIAN PHONE NUMBER	Click here to enter text.
DATA CUSTODIAN EMAIL ADDRESS	Click here to enter text

PRA Disclosure Statement

According to the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number. The valid OMB control number for this information collection is **0938-1411 (Expires 02/28/2025)**. This is a **required to retain or obtain a benefit** information collection. The time required to complete this information collection is estimated to average **90 minutes** per response, including the time to review instructions, search existing data resources, gather the data needed, and complete and review the information collection. If you have comments concerning the accuracy of the time estimate(s) or suggestions for improving this form, please write to: CMS, 7500 Security Boulevard, Attn: PRA Reports Clearance Officer, Mail Stop C4-26-05, Baltimore, Maryland 21244-1850. ****CMS Disclosure**** **Please do not send applications, claims, payments, medical records or any documents containing sensitive information to the PRA Reports Clearance Office. Please note that any correspondence not pertaining to the information collection burden approved under the associated OMB control number listed on this form will not be reviewed, forwarded, or retained. If you have questions or concerns regarding where to submit your documents, please contact DataUseAgreement@cms.hhs.gov.**

Please provide the information for a secondary Point of Contact (POC) in the event the Data Custodian changes or cannot be reached.

SECONDARY POC	Click here to enter text.
SECONDARY POC PHONE NUMBER	Click here to enter text.
SECONDARY POC EMAIL ADDRESS	Click here to enter text

3. INSTRUCTIONS FOR COMPLETING THE DMP SAQ

The DMP SAQ contains security and privacy controls based on the CMS Acceptable Risk Safeguards 3.1 Publication, which uses NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* control reference structure. Please note that below each question the CMS Acceptable Risk Safeguards 3.1 Publication safeguard number has been provided for reference, if additional guidance is needed.

For Section 4 (Security Controls): A security control is defined as an operational, technical, or management safeguard or countermeasure used by an information system or an organization to maintain the integrity, confidentiality, and availability of its information.

- For each question, in Part A (i.e., 1A, 2A, etc.), please:
  - Answer "Yes" if the security control is documented in a policy or procedure and all elements of the question are satisfied.
  - Answer "No" if the security control is not documented in a policy or procedure or if all elements of the question are not satisfied.
- In Part A, please note that a rationale is required for both "Yes" and "No" responses.
  - If "Yes," please cite the documentation and describe the capability.
  - If "No," please provide a rationale and any compensating control(s) in effect.
- In Part B, please note that a rationale is optional.
- **Rationale and policies:** A rationale or policy reference is required for all Part A questions in Section 4. Please note that a rationale is optional for all Part B questions. A rationale should reference or describe the method by which a control will be addressed by the DUA requesting organization or indicate the compensating security control(s) in place. The National Institute of Standards and Technology (NIST) defines a compensating security control as a management, operational, or technical control used by an organization instead of a recommended security control that provides equivalent or comparable protection for an information system.

For Section 5 (Privacy Controls): As defined by the National Institute of Standards and Technology (NIST), a privacy control is an administrative, technical, and physical safeguard employed within an organization to protect and ensure the proper handling of PII or prevent activities that create privacy risks.

- For this section, provide an attestation of "Yes" or "No" if the control has been implemented at your organization. Please note that none of the questions require a rationale, any rationale provided in Section 5 is optional.

GUIDANCE: For supplementary guidance on the CMS ARS requirements for privacy and security controls, please refer to the Data Management Plan Self-Attestation Questionnaire (DMP SAQ): Requirements & Guidance for Security & Privacy Controls.

4. SECURITY CONTROLS

1A. Access Controls: Attestation and Rationale

#	Question	Response
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)	☐ Yes ☐ No
	Click here to enter rationale (*Required*).	
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)	☐ Yes ☐ No
	Click here to enter rationale (*Required*).	
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)	☐ Yes ☐ No
	Click here to enter rationale (*Required*).	
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)	☐ Yes ☐ No
	Click here to enter rationale (*Required*).	

1B. Access Controls: Attestation

#	Question	Response
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)	☐ Yes ☐ No
	Click here to enter text (*Optional*).	
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)	☐ Yes ☐ No
	Click here to enter text (*Optional*).	

#	Question	Response
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))	☐ Yes ☐ No
	Click here to enter text (*Optional*).	
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)	☐ Yes ☐ No
	Click here to enter text (*Optional*).	
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)	☐ Yes ☐ No
	Click here to enter text (*Optional*).	
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)	☐ Yes ☐ No
	Click here to enter text (*Optional*).	
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)	☐ Yes ☐ No
	Click here to enter text (*Optional*).	
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))	☐ Yes ☐ No
	Click here to enter text (*Optional*).	
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))	☐ Yes ☐ No

#	Question	Response
	Click here to enter text (*Optional*).	
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))	☐ Yes ☐ No
	Click here to enter text (*Optional*).	
1.15	Does your organization have a process for determining what is shared with external users (e.g. collaborators)? (ARS v3.1 AC-21)	☐ Yes ☐ No
	Click here to enter text (*Optional*).	

2A. Awareness and Training Controls: Attestation and Rationale

#	Question	Response
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)	☐ Yes ☐ No
	Click here to enter rationale (*Required*).	
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)	☐ Yes ☐ No
	Click here to enter rationale (*Required*).	

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	Response
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)	☐ Yes ☐ No
	Click here to enter rationale (*Required*).	
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)	☐ Yes ☐ No
	Click here to enter rationale (*Required*).	
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))	☐ Yes ☐ No
	Click here to enter rationale (*Required*).	

3B. Auditing and Accountability Controls: Attestation

#	Question	Response
3.4	Does your organization ensure adequate storage capacity for 90 days of audit records? (ARS v3.1 AU-04, AU-11)	☐ Yes ☐ No
	Click here to enter text (*Optional*).	
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)	☐ Yes ☐ No
	Click here to enter text (*Optional*).	

#	Question	Response
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))	☐ Yes ☐ No
	Click here to enter text (*Optional*).	
3.7	Does your organization ensure audit records are searchable? (ARS v3.1 AU-07(01), AU-07(02))	☐ Yes ☐ No
	Click here to enter text (*Optional*).	
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))	☐ Yes ☐ No
	Click here to enter text (*Optional*).	
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))	☐ Yes ☐ No
	Click here to enter text (*Optional*).	
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)	☐ Yes ☐ No
	Click here to enter text (*Optional*).	

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

#	Question	Response
4.1	Does your organization have a policy for security assessment and authorization activities? (ARS v3.1 CA-01)	☐ Yes ☐ No
	Click here to enter rationale (*Required*).	
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	☐ Yes ☐ No

#	Question	Response
	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)	
	Click here to enter rationale (*Required*).	
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))	☐ Yes ☐ No
	Click here to enter rationale (*Required*).	

4B. Security Assessment and Authorization Controls: Attestation

#	Question	Response
4.4	Does your organization have a continuous monitoring program that manages identified vulnerabilities, remediation and ongoing security assessments? (ARS v3.1 CA-07)	☐ Yes ☐ No
	Click here to enter text (*Optional*).	

5A. Configuration Management Controls: Attestation and Rationale

#	Question	Response
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)	☐ Yes ☐ No
	Click here to enter rationale (*Required*).	
5.2	Does your organization track, review, approve or disapprove, and log changes to organizational information systems? (ARS v3.1 CM-03)	☐ Yes ☐ No
	Click here to enter rationale (*Required*).	
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)	☐ Yes ☐ No
	Click here to enter rationale (*Required*).	

5B. Configuration Management Controls: Attestation

#	Question	Response
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)	☐ Yes ☐ No
	Click here to enter text (*Optional*).	
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)	☐ Yes ☐ No
	Click here to enter text (*Optional*).	
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)	☐ Yes ☐ No
	Click here to enter text (*Optional*).	
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))	☐ Yes ☐ No
	Click here to enter text (*Optional*).	
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)	☐ Yes ☐ No
	Click here to enter text (*Optional*).	

6A. Contingency Planning Controls: Attestation and Rationale

#	Question	Response
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)	☐ Yes ☐ No

#	Question	Response
	Click here to enter rationale (*Required*).	
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)	☐ Yes ☐ No
	Click here to enter rationale (*Required*).	

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	Response
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)	☐ Yes ☐ No
	Click here to enter rationale (*Required*).	
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)	☐ Yes ☐ No
	Click here to enter rationale (*Required*).	

7B. Identification and Authentication Controls: Attestation

#	Question	Response
7.3	Does your organization's information system use unique identifiers for users and scheduled processes (e.g., backups)? (ARS v3.1 IA-02)	☐ Yes ☐ No
	Click here to enter text (*Optional*).	
7.4	Does your organization ensure the information system uniquely identifies devices (e.g., IP address, hostname, etc.)?	☐ Yes ☐ No

#	Question	Response
	(ARS v3.1 IA-03)	
	Click here to enter text (*Optional*).	
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)	☐ Yes ☐ No
	Click here to enter text (*Optional*).	
7.6	Does your organization ensure the information system shows non-descript information when authentication fails? (ARS v.3.1 IA-06)	☐ Yes ☐ No
	Click here to enter text (*Optional*).	

8A. Incident Response Controls: Attestation and Rationale

#	Question	Response
8.1	Does your organization have an incident response policy that is reviewed/updated at least once a year? (ARS v3.1 IR-01)	☐ Yes ☐ No
	Click here to enter rationale (*Required*).	
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)	☐ Yes ☐ No
	Click here to enter rationale (*Required*).	

8B. Incident Response Controls: Attestation

#	Question	Response
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)	☐ Yes ☐ No
	Click here to enter text (*Optional*).	
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)	☐ Yes ☐ No

#	Question	Response
	Click here to enter text (*Optional*).	
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)	☐ Yes ☐ No
	Click here to enter text (*Optional*).	
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)	☐ Yes ☐ No
	Click here to enter text (*Optional*).	
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, 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)	☐ Yes ☐ No
	Click here to enter text (*Optional*).	

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	Response
9.1	Does your organization have a system maintenance policy that is reviewed/updated at least once a year? (ARS v3.1 MA-01)	☐ Yes ☐ No
	Click here to enter text (*Optional*).	

#	Question	Response
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))	☐ Yes ☐ No
	Click here to enter text (*Optional*).	
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))	☐ Yes ☐ No
	Click here to enter text (*Optional*).	

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	Response
10.1	Does your organization have a media protection policy that is reviewed/updated at least once a year? (ARS v3.1 MP-01)	☐ Yes ☐ No
	Click here to enter text (*Optional*).	
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)	☐ Yes ☐ No
	Click here to enter text (*Optional*).	
10.3	Does your organization protect and securely stores digital media and ensure it is overwritten once with a "00000000x" pattern or degaussed with a NIST approved degaussing device? (ARS v3.1 MP-04, MP-06)	☐ Yes ☐ No
	Click here to enter text (*Optional*).	
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	☐ Yes ☐ No

#	Question	Response
	media; and restricts the activities associated with the transport of information system media to authorized personnel? (ARS v3.1 MP-05)	
	Click here to enter text (*Optional*).	
10.5	Does your organization sanitize media prior to disposal or reuse and track such activities? (ARS v3.1 MP-06, MP-06(01))	☐ Yes ☐ No
	Click here to enter text (*Optional*).	
10.6	Does your organization prohibit the use of personally owned media? (ARS v3.1 MP-07, MP-07(01))	☐ Yes ☐ No
	Click here to enter text (*Optional*).	
10.7	Does your organization ensure that any portable media devices have an identified owner? (ARS v3.1 MP 07, MP-07(01))	☐ Yes ☐ No
	Click here to enter text (*Optional*).	
10.8	Does your organization ensure that records of disposed media which contain sensitive information are maintained? (ARS v3.1 MP-CMS-01)	☐ Yes ☐ No
	Click here to enter text (*Optional*).	

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	Response
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)	☐ Yes ☐ No
	Click here to enter text (*Optional*).	
11.2	Does your organization maintain a current list of authorized individuals to enter the facility? (ARS v3.1 PE-02)	☐ Yes ☐ No
	Click here to enter text (*Optional*).	

#	Question	Response
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)	☐ Yes ☐ No
	Click here to enter text (*Optional*).	
11.4	Does your organization ensure that telephone and network hardware and transmission lines are protected? (ARS v3.1 PE-04)	☐ Yes ☐ No
	Click here to enter text (*Optional*).	
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)	☐ Yes ☐ No
	Click here to enter text (*Optional*).	

12A. Planning Controls: Attestation and Rationale

#	Question	Response
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)	☐ Yes ☐ No
	Click here to enter rationale (*Required*).	
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)	☐ Yes ☐ No
	Click here to enter rationale (*Required*).	

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	Response
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)	☐ Yes ☐ No
	Click here to enter text (*Optional*).	
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 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)	☐ Yes ☐ No
	Click here to enter text (*Optional*).	
13.3	Does your organization have processes for re-screening personnel according to organizationally defined conditions as required? (ARS v3.1 PS-03)	☐ Yes ☐ No
	Click here to enter text (*Optional*).	
13.4	Does your organization ensure that users sign access agreements every 365 days? (ARS v3.1 PS-06)	☐ Yes ☐ No
	Click here to enter text (*Optional*).	
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)	☐ Yes ☐ No
	Click here to enter text (*Optional*).	
13.6	Does your organization ensure that the organization has a formal sanction process for employees who violate security policies or procedures?	☐ Yes ☐ No

#	Question	Response
	(ARS v3.1 PS-08)	
	Click here to enter text (*Optional*).	

14A. Risk Assessment Controls: Attestation and Rationale

#	Question	Response
14.1	Does your organization utilize an automated vulnerability scanner in compliance with organizational policies? How is this performed? (ARS v3.1 RA-05)	☐ Yes ☐ No
	Click here to enter rationale (*Required*).	

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	Response
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)	☐ Yes ☐ No
	Click here to enter text (*Optional*).	
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)	☐ Yes ☐ No
	Click here to enter text (*Optional*).	
15.3	Does your organization ensure that any external services (third-party ticketing, messaging, auditing, monitoring, etc.) outside of the accreditation/authorization boundary comply with organizational information security requirements?	☐ Yes ☐ No

#	Question	Response
	(ARS v3.1 SA-09)	
	Click here to enter text (*Optional*).	

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

#	Question	Response
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)	☐ Yes ☐ No
	Click here to enter rationale (*Required*).	
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)	☐ Yes ☐ No
	Click here to enter rationale (*Required*).	

16B. System and Communications Protection Controls: Attestation

#	Question	Response
16.3	Does your organization ensure that administrative and regular user interfaces are separate? (ARS v3.1 SC-02)	☐ Yes ☐ No
	Click here to enter text (*Optional*).	
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)	☐ Yes ☐ No
	Click here to enter text (*Optional*).	
16.5	Does your organization have a centralized cryptographic key management system that complies with organizational standards? (ARS v3.1 SC-12)	☐ Yes ☐ No
	Click here to enter text (*Optional*).	
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)	☐ Yes ☐ No
	Click here to enter text (*Optional*).	

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

#	Question	Response
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)	☐ Yes ☐ No
	Click here to enter rationale (*Required*).	
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))	☐ Yes ☐ No
	Click here to enter rationale (*Required*).	
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)	☐ Yes ☐ No
	Click here to enter rationale (*Required*).	

17B. System and Information Integrity Controls: Attestation

#	Question	Response
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)	☐ Yes ☐ No
	Click here to enter text (*Optional*).	
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)	☐ Yes ☐ No
	Click here to enter text (*Optional*).	
17.6	Are email servers being hosted by the organization in the authorization boundary? Are spam filters used with the mail servers?	☐ Yes ☐ No

#	Question	Response
	(ARS v3.1 SI-08)	
	Click here to enter text (*Optional*).	
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)	☐ Yes ☐ No
	Click here to enter text (*Optional*).	
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)	☐ Yes ☐ No
	Click here to enter text (*Optional*).	

18A. Program Management Controls: Attestation and Rationale

#	Question	Response s
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)	☐ Yes ☐ No
	Click here to enter rationale (*Required*).	

18B. Program Management Controls: Attestation

Please note that there are no questions in this control family that require an attestation. Please proceed to the Section 5: Privacy Controls.

5. PRIVACY CONTROLS

19. Accountability, Audit and Risk Management

#	Question	Response
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)	☐ Yes ☐ No
	Click here to enter text (*Optional*).	
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)	☐ Yes ☐ No
	Click here to enter text (*Optional*).	
19.3	Does your organization monitor privacy policies and audit privacy controls at least once every year? (ARS v3.1 AR-04)	☐ Yes ☐ No
	Click here to enter text (*Optional*).	
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)	☐ Yes ☐ No
	Click here to enter text (*Optional*).	
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)	☐ Yes ☐ No
	Click here to enter text (*Optional*).	
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)	☐ Yes ☐ No
	Click here to enter text (*Optional*).	

#	Question	Response
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)	☐ Yes ☐ No
	Click here to enter text (*Optional*).	

20. Authority and Purpose

#	Question	Response
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)	☐ Yes ☐ No
	Click here to enter text (*Optional*).	

21. Data Minimization and Retention

#	Question	Response
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)	☐ Yes ☐ No
	Click here to enter text (*Optional*).	

22. Data Quality and Integrity

#	Question	Response
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)	☐ Yes ☐ No
	Click here to enter text (*Optional*).	

23. Individual Participation and Redress

#	Question	Response
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)	☐ Yes ☐ No
	Click here to enter text (*Optional*).	

24. Security

#	Question	Response
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)	☐ Yes ☐ No
	Click here to enter text (*Optional*).	

25. Transparency

#	Question	Response
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)	☐ Yes ☐ No
	Click here to enter text (*Optional*).	

26. Use Limitation

#	Question	Response
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)	☐ Yes ☐ No
	Click here to enter text (*Optional*).	

#	Question	Response
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)	☐ Yes ☐ No
	Click here to enter text (*Optional*).	
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)	☐ Yes ☐ No
	Click here to enter text (*Optional*).	

6. DATA CUSTODIAN ATTESTATION

a) I acknowledge my appointment as Data Custodian on behalf of the requesting organization and agree to comply with the provisions of any Data Use Agreement (DUA) with CMS where I am listed as the Data Custodian.
b) As the Data Custodian, it is my responsibility to monitor the DUAs that cover data stored in the environment listed in section 1 of this DMP SAQ.
c) As the Data Custodian, it is my responsibility to monitor the data recipients who receive CMS data and load the data into the environment listed in section 1 of this DMP SAQ.
d) All of the information provided in this DMP SAQ is accurate, true, and complete to the best of my knowledge.
e) I must notify the Data Privacy Safeguard Program (DPSP) of any changes to the information provided in this Data Management Plan Self-Attestation Questionnaire (DMP SAQ) within fifteen (15) days at data_privacy_safeguard_program@mbltechnologies.com.
f) I further understand that any false information may result in the denial or revocation of my organization's Data Use Agreements (DUAs).

Signature: _____ **Date:** _____

FOR OFFICE USE ONLY	
DMP SAQ Approval Date	
DMP SAQ Expiration Date	