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 5.1 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

Individual who will be responsible for ensuring that the environment in which the CMS data is stored complies with all applicable CMS data security requirements, 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.

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

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 5.1 Publication, which uses NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations* control reference structure. Please note that for each question the CMS Acceptable Risk Safeguards 5.1 Publication safeguard number has been provided for reference.

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 (e.g., 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. o 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 for "Yes" responses. A rationale is required for "No" responses.
- 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.

GUIDANCE: For supplementary guidance on the CMS Acceptable Risk Safeguards requirements for privacy and security controls, please refer to the Data Management Plan Self-Attestation Questionnaire (DMP SAQ) website.

4. SECURITY AND PRIVACY 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 and is the policy disseminated to the appropriate personnel or roles? (Acceptable Risk Safeguards 5.1 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, review user accounts periodically, and notify account managers within 30 days when accounts are no longer required or when system users are terminated or transferred? (Acceptable Risk Safeguards 5.1 AC-02)	☐ Yes ☐ No
	Click here to enter rationale. (*Required*)	
#	**Question**	**Response**
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. (Acceptable Risk Safeguards 5.1 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? (Acceptable Risk Safeguards 5.1 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? (Acceptable Risk Safeguards 5.1 AC-03)	☐ Yes ☐ No
	Click here to enter rationale. (*Optional if response is "Yes." Required if response is "No.")*	
1.6	Does your organization's information system separate users based on their duties (e.g., users, researchers, management, etc.)? (Acceptable Risk Safeguards 5.1 AC-05)	☐ Yes ☐ No
	Click here to enter rationale. (*Optional if response is "Yes." Required if response is "No.")*	
1.7	Does your organization ensure that only authorized users have permissions required to perform their job functions by disabling non-essential functions and removable media devices; ensure security functions are explicitly authorized; ensure that authorized users utilize their own account to access the system; escalate privileges to perform administrative functions; and log all privileged account usage activities? (Acceptable Risk Safeguards 5.1 AC-06, AC-06(01), AC-06(09))	☐ Yes ☐ No
	Click here to enter rationale. (*Optional if response is "Yes." Required if response is "No.")*	

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. (Acceptable Risk Safeguards 5.1 AC-07)	☐ Yes ☐ No
	Click here to enter rationale. (*Optional if response is "Yes." Required if response is "No.")*	
1.9	Does your organization's information system display a notification or banner before granting access to the information systems?	☐ Yes ☐ No
#	**Question**	**Response**
	(Acceptable Risk Safeguards 5.1 AC-08)	
	Click here to enter rationale. (*Optional if response is "Yes." Required if response is "No.")*	
1.10	Does your organization's information system lock user devices after an organization defined time limit of inactivity and require the user to initiate a device lock before leaving the system unattended? Does it retain the device lock until the user reestablishes access using established identification and authentication procedures? (Acceptable Risk Safeguards 5.1 AC-11)	☐ Yes ☐ No
	Click here to enter rationale. (*Optional if response is "Yes." Required if response is "No.")*	
1.11	Does your organization identify actions (defined in applicable security and privacy plans) that can be taken on the system without identification or authentication (e.g., viewing certain webpages with public information only or generic information)? (Acceptable Risk Safeguards 5.1 AC-14)	☐ Yes ☐ No
	Click here to enter rationale. (*Optional if response is "Yes." Required if response is "No.")*	
1.12	Do your organization's remote connections have usage restrictions; connection requirements such as cryptography connected to managed network access control points; and guidelines for user access? Are they monitored through audit records and explicitly authorize the usage of privileged commands through the remote connection? (Acceptable Risk Safeguards 5.1 AC-17, AC-17(01), AC-17(02), AC-17(03), AC-17(04))	☐ Yes ☐ No
	Click here to enter rationale. (*Optional if response is "Yes." Required if response is "No.")*	
1.13	Does your organization establish configuration requirements, connection requirements, and implementation guidance for wireless access and/or mobile devices? (Acceptable Risk Safeguards 5.1 AC-18, AC-19)	☐ Yes ☐ No
	Click here to enter rationale. (*Optional if response is "Yes." Required if response is "No.")*	
1.14	Does your organization ensure that the information system does not allow external systems to process, store, or transmit system information unless explicitly authorized? (Acceptable Risk Safeguards 5.1 AC-20, AC-20(01), AC-20(02))	☐ Yes ☐ No
	Click here to enter rationale. (*Optional if response is "Yes." Required if response is "No.")*	

1.15	Does your organization have a process for determining what is shared with external users (e.g., collaborators)? (Acceptable Risk Safeguards 5.1 AC-21)	☐ Yes ☐ No
	Click here to enter rationale. (*Optional if response is "Yes." Required if response is "No."*)	

2A. Awareness and Training Controls: Attestation and Rationale

#	Question	Response
2.1	Does your organization ensure that system users (including managers, senior executives, and contractors) receive security and privacy literacy training as part of initial training of new users, annually thereafter, and when required by system changes or events as defined by the organization; and that such users certify manually or electronically completion of training? (Acceptable Risk Safeguards 5.1 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 or privacy related duties and responsibilities prior to them assuming their security or privacy specific roles and responsibilities? Do they receive additional training based on system changes (e.g., statute, regulation, or policy changes) and at least once a year for refreshed role-based security and privacy training? (Acceptable Risk Safeguards 5.1 AT-03)	☐ Yes ☐ No
	Click here to enter rationale. (*Required*)	

2B. Awareness and Training Controls

Please note that there are no questions in this section. 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 and is the policy disseminated to the appropriate personnel or roles? (Acceptable Risk Safeguards 5.1 AU-01)	☐ Yes ☐ No
	Click here to enter rationale. (*Required*)	

3.2	Does your organization's information system have the capability to log events in support of the audit function including: User logon and logoff (successful and unsuccessful); all system administration activities; modification of privileges and access; application alerts and error messages; configuration changes, account creation; modification or deletion; concurrent logon from different workstations; override of access control mechanisms; startup/shutdown of audit logging services; and audit logging service configuration changes? (Acceptable Risk Safeguards 5.1 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:	☐ Yes ☐ No
#	**Question**	**Response**
	Date and time of the event (e.g., timestamp); process identifier or system component (e.g., software, hardware) generating the event; user or account that initiated the event (unique username/identifier); event type; event outcome (success/failure); any privileged system functions executed; process creation information (command line captures if applicable)? (Acceptable Risk Safeguards 5.1 AU-03, AU-03(01))	
	Click here to enter rationale. (*Required*)	

3B. Auditing and Accountability Controls: Attestation

#	Question	Response
3.4	Does your organization ensure adequate storage capacity to reduce the likelihood of such capacity being exceeded? (Acceptable Risk Safeguards 5.1 AU-04)	☐ Yes ☐ No
	Click here to enter rationale. (*Optional if response is "Yes." Required if response is "No.")*	
3.5	Does your organization ensure that administrators are notified of process failures through the audit logging process of the information systems? (Acceptable Risk Safeguards 5.1 AU-05)	☐ Yes ☐ No
	Click here to enter rationale. (*Optional if response is "Yes." Required if response is "No.")*	
3.6	Does your organization ensure that: Audit records are reviewed weekly; system logs, network utilization/traffic, security software, and alerts are reviewed daily; automated audit record analysis is used to review audit records; automated audit record analysis is correlated across the organization; and administrator groups logs are inspected at least every 14 days to ensure unauthorized administrator, system, and privileged application accounts have not been created? (Acceptable Risk Safeguards 5.1 AU-06, AU-06(03))	☐ Yes ☐ No
	Click here to enter rationale. (*Optional if response is "Yes." Required if response is "No.")*	

3.7	Does your organization ensure audit records are searchable? (Acceptable Risk Safeguards 5.1 AU-07(01))	☐ Yes ☐ No
	Click here to enter rationale. (*Optional if response is "Yes." Required if response is "No.")*	
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? (Acceptable Risk Safeguards 5.1 AU-08)	☐ Yes ☐ No
	Click here to enter rationale. (*Optional if response is "Yes." Required if response is "No.")*	
#	**Question**	**Response**
3.9	Does your organization ensure that audit information and audit logging tools are protected from unauthorized access, deletion, and modification? Is access to the management of audit logging functionality limited to a subset of privileged users? (Acceptable Risk Safeguards 5.1 AU-09, AU-09(04))	☐ Yes ☐ No
	Click here to enter rationale. (*Optional if response is "Yes." Required if response is "No.")*	
3.10	Does your organization ensure that audit records are retained for 90 days in "hot" storage and retained for one year in archive storage? (Acceptable Risk Safeguards 5.1 AU-11)	☐ Yes ☐ No
	Click here to enter rationale. (*Optional if response is "Yes." Required if response is "No.")*	

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

#	Question	Response
4.1	Does your organization have a policy for assessment, authorization, and monitoring activities that is reviewed/updated at least once a year or whenever there is a significant system modification and is the policy disseminated to the appropriate personnel or roles? (Acceptable Risk Safeguards 5.1 CA-01)	☐ Yes ☐ No
	Click here to enter rationale. (*Required*)	
4.2	Does your organization approve and manage the exchange of information between the system and other systems where CMS data resides and document, as part of exchange agreements, the security and privacy requirements, controls, and responsibilities of each system? (Acceptable Risk Safeguards 5.1 CA-03, CA-09)	☐ Yes ☐ No
	Click here to enter rationale. (*Required*)	

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

#	Question	Response
4.3	Does your organization have a continuous monitoring program that manages identified vulnerabilities, remediation, and ongoing security and privacy assessments and reports the security and privacy status of the system to appropriate personnel or roles? (Acceptable Risk Safeguards 5.1 CA-07)	☐ Yes ☐ No
	Click here to enter rationale. (*Optional if response is "Yes." Required if response is "No.")*	

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 or whenever there is a significant system modification and is the policy disseminated to the appropriate personnel or roles? (Acceptable Risk Safeguards 5.1 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 with explicit consideration for security and privacy impact analyses? (Acceptable Risk Safeguards 5.1 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? (Acceptable Risk Safeguards 5.1 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 system components within the information system and review and update the baseline configuration at least once a year, when required due to major system changes/updates, or when system components are installed or upgraded? (Acceptable Risk Safeguards 5.1 CM-02)	☐ Yes ☐ No
	Click here to enter rationale. (*Optional if response is "Yes." Required if response is "No.")*	

5.5	Does your organization ensure that the information system uses physical and logical access restrictions to prevent unauthorized changes to the information systems? (Acceptable Risk Safeguards 5.1 CM-05)	☐ Yes ☐ No
	Click here to enter rationale. (*Optional if response is "Yes." Required if response is "No.")*	
5.6	Does your organization ensure that the configuration of the information system allows only essential functions, software, ports, protocols, and applications? (Acceptable Risk Safeguards 5.1 CM-07)	☐ Yes ☐ No
	Click here to enter rationale. (*Optional if response is "Yes." Required if response is "No.")*	
5.7	Does your organization maintain and review at least every 180 days an up-to-date system inventory of metadata to include all boundary components, such as:	☐ Yes ☐ No
#	**Question**	**Response**
	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? (Acceptable Risk Safeguards 5.1 CM-08, CM-08(01))	
	Click here to enter rationale. (*Optional if response is "Yes." Required if response is "No.")*	
5.8	Does your organization ensure that the information system prevents users from installing non-approved software through user policies? (Acceptable Risk Safeguards 5.1 CM-11)	☐ Yes ☐ No
	Click here to enter rationale. (*Optional if response is "Yes." Required if response is "No.")*	

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 or when there is a significant system modification and is the policy disseminated to the appropriate personnel or roles? Does your organization's contingency planning include coordination with organizational elements responsible for related plans (e.g., Business Continuity Plans, Disaster Recovery Plans, Critical Infrastructure Plans, Continuity of Operations Plans, etc.)? (Acceptable Risk Safeguards 5.1 CP-01, CP-02(01))	☐ Yes ☐ No
	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 and privacy related documentation? How does your organization protect the confidentiality, integrity, and availability of backups containing CMS data? (Acceptable Risk Safeguards 5.1 CP-09)	☐ Yes ☐ No
	Click here to enter rationale. (*Required*)	

6B. Contingency Planning Controls: Attestation

Please note that there are no questions in this section. 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 or when there is a significant system modification and is the policy disseminated to the appropriate personnel or roles? (Acceptable Risk Safeguards 5.1 IA-01)	☐ Yes ☐ No
	Click here to enter rationale. (*Required*)	
7.2	Does your organization uniquely identify and authenticate users, processes, or devices prior to granting access to organizational systems through effective identity proofing and authentication processes? Describe how your organization establishes initial content for authenticators; defines reuse conditions; and sets minimum and maximum lifetimes for each authenticator type to be used. (Acceptable Risk Safeguards 5.1 IA-02, IA-03, IA-05, IA-12)	☐ 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)? (Acceptable Risk Safeguards 5.1 IA-02)	☐ Yes ☐ No
	Click here to enter rationale. (*Optional if response is "Yes." Required if response is "No.")*	
7.4	Does your organization ensure the information system uniquely identifies devices (e.g., IP address, hostname, etc.)? (Acceptable Risk Safeguards 5.1 IA-03)	☐ Yes ☐ No
	Click here to enter rationale. (*Optional if response is "Yes." Required if response is "No.")*	

7.5	Does your organization successfully assign unique identifiers to users and devices; prevent reuse of identifiers for three years or verify that access to sensitive information is removed prior to any reuse; and disable identifiers after 60 days of inactivity? (Acceptable Risk Safeguards 5.1 IA-04)	☐ Yes ☐ No
	Click here to enter rationale. (*Optional if response is "Yes." Required if response is "No.")*	
7.6	Does your organization ensure the information system shows non-descript information when authentication fails? (Acceptable Risk Safeguards 5.1 IA-06)	☐ Yes ☐ No
	Click here to enter rationale. (*Optional if response is "Yes." Required if response is "No.")*	

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 or when there is a significant system modification and is the policy disseminated to the appropriate personnel or roles? (Acceptable Risk Safeguards 5.1 IR-01)	☐ Yes ☐ No
	Click here to enter rationale. (*Required*)	
8.2	Does your organization investigate incidents (e.g., preparation, detection, analysis, containment, eradication, and recovery); consistently track and monitor incidents (e.g., physical, technical, and privacy); and ensure that the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization? Describe how your organization investigates incidents. (Acceptable Risk Safeguards 5.1 IR-04, IR-05)	☐ Yes ☐ No
	Click here to enter rationale. (*Required*)	
8.3	Regarding data breaches, can your organization attest that there have been no breaches affecting 500 or more data subjects reported to the HHS Office for Civil Rights within the last 2 years? If there has been a breach, please provide the nature and date of the breach. (Acceptable Risk Safeguards 5.1 IR-08(01))	☐ Yes ☐ No
	Click here to enter rationale. (*Required*)	

8B. Incident Response Controls: Attestation

#	Question	Response
8.4	Does your organization ensure that employees who have incident response duties complete incident response training within one month of assuming the role and annually thereafter and that incident response training content is reviewed and updated annually? (Acceptable Risk Safeguards 5.1 IR-02)	☐ Yes ☐ No

	Click here to enter rationale. (*Optional if response is "Yes." Required if response is "No."*)	
8.5	Does your organization have the capability to investigate incidents (e.g., physical, technical and privacy), that includes preparation, detection, analysis, containment, eradication, and recovery and ensure that the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization? (Acceptable Risk Safeguards 5.1 IR-04, IR-05)	☐ Yes ☐ No
	Click here to enter rationale. (*Optional if response is "Yes." Required if response is "No."*)	
8.6	Does your organization have incident response resources that can assist system administrators (e.g., help desks, assistance groups, access to forensics services, etc.) for the handling and reporting of security and privacy incidents? (Acceptable Risk Safeguards 5.1 IR-07)	☐ Yes ☐ No
	Click here to enter rationale. (*Optional if response is "Yes." Required if response is "No."*)	
#	**Question**	**Response**
8.7	Does your organization have an incident response plan that: Provides the organization with a roadmap for implementing its incident response capability; describes the structure and organization of the incident response capability; provides a high-level approach for how the incident response capability fits into the overall organization; meets the unique requirements of the organization, which relate to mission, size, structure, and functions; defines reportable incidents; provides metrics for measuring the incident response capability within the organization; defines the resources and management support needed to effectively maintain and mature an incident response capability; is reviewed and approved by the applicable Incident Response Team Leader; is distributed to the organization's information security officers and other incident response team personnel; is reviewed within every 365 days or when an IR event(s) demonstrates a change and/or update is needed to improve the IR Plan; is updated to address system/organizational changes or problems encountered during plan implementation, execution, or testing; communicate incident response plan changes to the organizational elements listed above; and is protected from unauthorized disclosure and modification? (Acceptable Risk Safeguards 5.1 IR-08)	☐ Yes ☐ No
	Click here to enter rationale. (*Optional if response is "Yes." Required if response is "No."*)	
8.8	Does your organization include in the incident response plan for breaches involving PII/PHI: A process to determine if notice to individuals or other organizations, including oversight organizations, is needed; an assessment process to determine the extent of harm, embarrassment, inconvenience, or unfairness to affected individuals and any mechanisms to mitigate such harms; and identification of any applicable privacy requirements. (Acceptable Risk Safeguards 5.1 IR-08(01))	☐ Yes ☐ No
	Click here to enter rationale. (*Optional if response is "Yes." Required if response is "No."*)	

9A. Maintenance Controls: Attestation and Rationale

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

9B. Maintenance Controls: Attestation

#	Question	Response
9.1	Does your organization have a system maintenance policy that is reviewed/updated at least once a year or when there is a significant system modification and is the policy disseminated to the appropriate personnel or roles? (Acceptable Risk Safeguards 5.1 MA-01)	☐ Yes ☐ No
	Click here to enter rationale. (*Optional if response is "Yes." Required if response is "No."*)	
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? (Acceptable Risk Safeguards 5.1 MA-03, MA-03(01))	☐ Yes ☐ No
#	**Question**	**Response**
	Click here to enter rationale. (*Optional if response is "Yes." Required if response is "No."*)	
9.3	Does your organization check media containing diagnostic and test programs being introduced into the system for malicious code, where applicable? (Acceptable Risk Safeguards 5.1 MA-03(02))	☐ Yes ☐ No
	Click here to enter rationale. (*Optional if response is "Yes." Required if response is "No."*)	

10A. Media Protection Controls: Attestation and Rationale

#	Question	Response
10.1	Does your organization have a media protection policy that is reviewed/updated at least once a year or when there is a significant system modification and is the policy disseminated to the appropriate personnel or roles? (Acceptable Risk Safeguards 5.1 MP-01)	☐ Yes ☐ No
	Click here to enter rationale. (*Required*)	
10.2	Does your organization prohibit the use of personally owned storage media? (Acceptable Risk Safeguards 5.1 MP-07)	☐ Yes ☐ No
	Click here to enter rationale. (*Required*)	
10.3	Does your organization ensure that any allowed portable storage devices have an owner (e.g., designated personnel or organization)? (Acceptable Risk Safeguards 5.1 MP-07)	☐ Yes identified ☐ No
	Click here to enter rationale. (*Required*)	

10.4	Does your organization protect and securely store digital media and ensure that any media with CMS data (including backups) is disposed of (e.g., clearing, purging, or destroying) in accordance with standards and policies, such as the latest revision of NIST SP 800-88, when such data is no longer required? (Acceptable Risk Safeguards 5.1 MP-04, MP-06)	☐ Yes ☐ No
	Click here to enter rationale. *(Required)*	

10B. Media Protection Controls: Attestation

#	Question	Response
10.5	Does your organization ensure the information system administrators mark system media based on the classification of information the media holds? (Acceptable Risk Safeguards 5.1 MP-03)	☐ Yes ☐ No
#	**Question**	**Response**
	Click here to enter rationale. (*Optional if response is "Yes." Required if response is "No.")*	
10.6	Does your organization protect media: While being transported, to include hand-carried – uses a securable container (e.g., locked briefcase) via authorized personnel; shipped – tracks with receipt by commercial carrier; maintains accountability for information system media during transport outside of controlled areas; documents activities associated with the transport of information system media; and restricts the activities associated with the transport of information system media to authorized personnel? (Acceptable Risk Safeguards 5.1 MP-05)	☐ Yes ☐ No
	Click here to enter rationale. (*Optional if response is "Yes." Required if response is "No.")*	
10.7	Does your organization sanitize media prior to disposal or reuse and track such activities? (Acceptable Risk Safeguards 5.1 MP-06, MP-06(01))	☐ Yes ☐ No
	Click here to enter rationale. *Optional if response is "Yes." Required if response is "No.")*	

11A. Physical and Environmental Controls: Attestation and Rationale

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

11B. Physical and Environmental Controls: Attestation

#	Question	Response
11.1	Does your organization have a physical and environmental policy that is reviewed/updated at least once a year or when there is a significant system modification and is the policy disseminated to the appropriate personnel or roles? (Acceptable Risk Safeguards 5.1 PE-01)	☐ Yes ☐ No

	Click here to enter rationale. (*Optional if response is "Yes." Required if response is "No."*)	
11.2	Does your organization maintain a current list of authorized individuals to enter the facility? (Acceptable Risk Safeguards 5.1 PE-02)	☐ Yes ☐ No
	Click here to enter rationale. (*Optional if response is "Yes." Required if response is "No."*)	
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	☐ Yes ☐ No
#	**Question**	**Response**
	(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? (Acceptable Risk Safeguards 5.1 PE-03)	
	Click here to enter rationale. (*Optional if response is "Yes." Required if response is "No."*)	
11.4	Does your organization ensure that telephone and network hardware and transmission lines are protected? (Acceptable Risk Safeguards 5.1 PE-04)	☐ Yes ☐ No
	Click here to enter rationale. (*Optional if response is "Yes." Required if response is "No."*)	
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? (Acceptable Risk Safeguards 5.1 PE-04)	☐ Yes ☐ No
	Click here to enter rationale. (*Optional if response is "Yes." Required if response is "No."*)	

12A. Planning Controls: Attestation and Rationale

#	Question	Response
12.1	Does your organization have a complete and up-to-date system security and privacy plan? How often is it reviewed/updated? Is it reviewed/updated to address changes to the information system and environment of operation? (Acceptable Risk Safeguards 5.1 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.) describe the responsibilities and expected behavior for information system usage, security and privacy and are signed by all users and administrators? Is this updated/reviewed at least once a year? How is it acknowledged? (Acceptable Risk Safeguards 5.1 PL-04)	☐ Yes ☐ No
	Click here to enter rationale. (*Required*)	

12B. Planning Controls: Attestation

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

13A. Personnel Security Controls: Attestation and Rationale

Please note that there are no questions in this section. Please proceed to 13B. **13B. Personnel Security Controls:** Attestation

#	Question	Response
13.1	Does your organization follow organizational policy regarding background checks and screening for employees with access to CMS data? (Acceptable Risk Safeguards 5.1 PS-03)	☐ Yes ☐ No
	Click here to enter rationale. (*Optional if response is "Yes." Required if response is "No."*)	
13.2	Does your organization upon termination of individual employment: Disable information system access before or during termination; terminate/revoke any authenticators/credentials associated with the individual; conduct exit interviews that include a discussion of non-disclosure of information security and privacy information; retrieve all security-related organizational information system-related property; retain access to organizational information and information systems formerly controlled by the terminated individual; notify defined personnel or roles (defined in the applicable security plan) within one calendar day; and immediately escort employees terminated for cause out of the organization? (Acceptable Risk Safeguards 5.1 PS-04)	☐ Yes ☐ No
	Click here to enter rationale. (*Optional if response is "Yes." Required if response is "No."*)	
13.3	Does your organization have processes for re-screening personnel according to organizationally defined conditions as required? (Acceptable Risk Safeguards 5.1 PS-03)	☐ Yes ☐ No
	Click here to enter rationale. (*Optional if response is "Yes." Required if response is "No."*)	
13.4	Does your organization ensure that users sign access agreements every 365 days? (Acceptable Risk Safeguards 5.1 PS-06)	☐ Yes ☐ No

	Click here to enter rationale. (*Optional if response is "Yes." Required if response is "No."*)	
13.5	Does your organization ensure that third-party service providers (contractors, CSPs, vendor maintenance) follow the same personnel requirements as full-time employees? (Acceptable Risk Safeguards 5.1 PS-07)	☐ Yes ☐ No
	Click here to enter rationale. (*Optional if response is "Yes." Required if response is "No."*)	
13.6	Does your organization ensure that the organization has a formal sanction process for employees who violate security policies or procedures? (Acceptable Risk Safeguards 5.1 PS-08)	☐ Yes ☐ No
	Click here to enter rationale. (*Optional if response is "Yes." Required if response is "No."*)	

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? (Acceptable Risk Safeguards 5.1 RA-05)	☐ Yes ☐ No
	Click here to enter rationale. (*Required*)	

14B. Risk Assessment Controls: Attestation

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

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

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

15B. System and Services Acquisition Controls: Attestation

#	Question	Response

15.1	Does your organization obtain or develop administrator documentation for the system or system components that describes: Secure configuration, installation, or operation; effective use and maintenance of security and privacy functions and mechanisms; and known vulnerabilities regarding configuration and use of administrative or privileged functions? (Acceptable Risk Safeguards 5.1 SA-05)	☐ Yes ☐ No
	Click here to enter rationale. (*Optional if response is "Yes." Required if response is "No.")*	
15.2	Does your organization acquire, develop, and manage the system using a system development life cycle (SDLC) process that incorporates information security and privacy considerations as well as apply security and privacy engineering principles in specification, design, development, implementation, and modification of the system and system components? (Acceptable Risk Safeguards 5.1 SA-03, SA-08)	☐ Yes ☐ No
	Click here to enter rationale. (*Optional if response is "Yes." Required if response is "No.")*	
15.3	Does your organization ensure that any external system services (third-party ticketing, messaging, auditing, monitoring, etc.) outside of the system boundary comply with organizational information security and privacy requirements?	☐ Yes ☐ No
#	**Question**	**Response**
	(Acceptable Risk Safeguards 5.1 SA-09)	
	Click here to enter rationale. (*Optional if response is "Yes." Required if response is "No.")*	

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 interfaces and key internal interfaces of organizational systems? What type of system is used? (Acceptable Risk Safeguards 5.1 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; Acceptable Risk Safeguards 5.1 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? (Acceptable Risk Safeguards 5.1 SC-02)	☐ Yes ☐ No
	Click here to enter rationale. (*Optional if response is "Yes." Required if response is "No."*)	
16.4	Does your organization's information system deny network communications traffic by default and allow network communications traffic by exception at managed interfaces or for specific systems? (Acceptable Risk Safeguards 5.1 SC-07(05))	☐ Yes ☐ No
	Click here to enter rationale. (*Optional if response is "Yes." Required if response is "No."*)	
16.5	Does your organization ensure that the information system terminates the network connection associated with a communications session at the end of the session or after a defined period of inactivity? (Acceptable Risk Safeguards 5.1 SC-10)	☐ Yes ☐ No
	Click here to enter rationale. (*Optional if response is "Yes." Required if response is "No."*)	
#	**Question**	**Response**
16.6	Does your organization have a centralized cryptographic key management system that complies with organizational standards? (Acceptable Risk Safeguards 5.1 SC-12)	☐ Yes ☐ No
	Click here to enter rationale. (*Optional if response is "Yes." Required if response is "No."*)	
16.7	Does your organization prohibit collaborative computing mechanisms (e.g., networked white boards, cameras, microphones, etc.) unless explicitly authorized? (Acceptable Risk Safeguards 5.1 SC-15)	☐ Yes ☐ No
	Click here to enter rationale. (*Optional if response is "Yes." Required if response is "No."*)	

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? (Acceptable Risk Safeguards 5.1 SI-03)	☐ Yes ☐ No
	Click here to enter rationale. (*Required*)	
17.2	Does your organization monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks? Is the monitoring used to identify unauthorized use of organizational systems? (Acceptable Risk Safeguards 5.1 SI-04, SI-04(04))	☐ Yes ☐ No

	Click here to enter rationale. (*Required*)	
17.3	Does your organization use file integrity monitoring (FIM) through employing tools and capabilities to monitor changes to critical resources such as operating system software components (e.g., OS images, kernel drivers, daemons), system firmware (e.g., the basic input/output system [BIOS]), and vital applications? (Acceptable Risk Safeguards 5.1 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 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? (Acceptable Risk Safeguards 5.1 SI-02)	☐ Yes ☐ No
	Click here to enter rationale. (*Optional if response is "Yes." Required if response is "No.")*	
17.5	Does your organization's information system use malicious code protection that has up-todate virus definitions and scans important file systems every 12 hours and full system every 72 hours? (Acceptable Risk Safeguards 5.1 SI-03)	☐ Yes ☐ No
	Click here to enter rationale. (*Optional if response is "Yes." Required if response is "No.")*	
17.6	Does your organization employ spam filters for email servers hosted within the system boundary, if applicable? (Acceptable Risk Safeguards 5.1 SI-08)	☐ Yes ☐ No
	Click here to enter rationale. (*Optional if response is "Yes." Required if response is "No.")*	
17.7	Does your organization's information system validate user input (e.g., username, password, or data entry fields) before accepting it into the system to protect against injection attacks, cross-site scripting, or other types of attacks? (Acceptable Risk Safeguards 5.1 SI-10)	☐ Yes ☐ No
	Click here to enter rationale. (*Optional if response is "Yes." Required if response is "No.")*	
17.8	Does your organization ensure the information systems retains information in accordance with federal law, CMS policy, and HIPAA requirements? (Acceptable Risk Safeguards 5.1 SI-12)	☐ Yes ☐ No
	Click here to enter rationale. (*Optional if response is "Yes." Required if response is "No.")*	

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? (Acceptable Risk Safeguards 5.1 PM-02)	☐ Yes ☐ No
	Click here to enter rationale. (*Required*)	

18B. Program Management Controls: Attestation

#	Question	Response s
18.2	Does your organization ensure that an accurate accounting of disclosures of PII is developed and maintained to include date, nature, and purpose of each disclosure; and contact information of the person or organization to which the disclosure was made? Does your organization also ensure that the accounting of disclosures is retained for the length the PII is maintained or five years after the disclosure is made, whichever is longer, and that the accounting of disclosures is made available to the related individual upon request? (Acceptable Risk Safeguards 5.1 PM-21)	☐ Yes ☐ No
	Click here to enter rationale. (*Optional if response is "Yes." Required if response is "No.")*	

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

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

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

#	Question	Response
19.1	Does your organization have a Personally Identifiable Information (PII) and Transparency policy that supports the security and privacy program and identifies the purpose, scope, roles, responsibilities, management commitment, and procedures to facilitate the implementation of the policy for the storage and processing of PII/PHI that is reviewed and updated at least every three (3) years or as needed? (Acceptable Risk Safeguards 5.1 PT-01)	☐ Yes ☐ No
	Click here to enter rationale. (*Optional if response is "Yes." Required if response is "No.")*	
19.2	Does your organization determine and document the relevant legal authority that permits the collection, use, maintenance, and sharing of PII/PHI and restrict the minimum relevant and necessary elements of PII/PHI to only that which is authorized? (Acceptable Risk Safeguards 5.1 PT-02)	☐ Yes ☐ No
	Click here to enter rationale. (*Optional if response is "Yes." Required if response is "No.")*	

19.3	Does your organization identify and document the purpose(s) for processing PII/PHI and restrict the processing of PII/PHI to only that which is compatible with the identified purpose(s)? (Acceptable Risk Safeguards 5.1 PT-03)	☐ Yes ☐ No
	Click here to enter rationale. (*Optional if response is "Yes." Required if response is "No.")*	
19.4	Does your organization apply defined processing conditions or protections as required by organizational policies and determinations for specific categories of PII/PHI, where applicable?	☐ Yes ☐ No
#	**Question**	**Response**
	(Acceptable Risk Safeguards 5.1 PT-07)	
	Click here to enter rationale. (*Optional if response is "Yes." Required if response is "No.")*	

20A. Supply Chain Risk Management Controls: Attestation and Rationale

Please note that there are no questions in this section. Please proceed to 20B.

20B. Supply Chain Risk Management Controls: Attestation

#	Question	Response
20.1	Does your organization develop a policy for the implementation of supply chain risk management and a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of the systems processing, transmitting, or storing CMS data? Are the policy and plan reviewed and updated annually or as required, to address environmental changes? (Acceptable Risk Safeguards 5.1 SR-01, SR-02)	☐ Yes ☐ No
	Click here to enter rationale. (*Optional if response is "Yes." Required if response is "No.")*	
20.2	Does your organization establish a process or processes to identify and address weaknesses or deficiencies in the supply chain elements and processes of systems processing, transmitting, or storing CMS data as well as assess and review supply chain-related risks associated with suppliers or contractor services on an annual basis? (Acceptable Risk Safeguards 5.1 SR-03, SR-06)	☐ Yes ☐ No
	Click here to enter rationale. (*Optional if response is "Yes." Required if response is "No.")*	
20.3	Does your organization dispose of CMS data and/or system components with CMS data using techniques and methods in accordance with the latest revision of NIST SP 800-88 (e.g., clearing, purging, destroying, or cryptographic erasure techniques for cloud components)? (Acceptable Risk Safeguards 5.1 SR-12)	☐ Yes ☐ No
	Click here to enter rationale. (*Optional if response is "Yes." Required if response is "No.")*	

5. 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 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 DMP SAQ to include any updates to the DUA Organization Information, Data Custodian, or Secondary POC within 15 days at DPSP@cms.hhs.gov.
f) I understand that submitting any false information or failing to meet the responsibilities listed above may result in the denial or revocation of my organization's DMP SAQ, denial or revocation of my organization's DUAs, and/or affect my organization's access to CMS data going forward.

Signature: _____ **Date:** _____

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