
# Qualified Entity Certification Program

# Data Security Review

# (QECP DSR)

**September 30, 2020**

**Final, Version 1.1**

**CMS Qualified Entity Certification Program**

**For CMS Use Only**

# Introduction to the QECP DSR

The Centers for Medicare & Medicaid Services (CMS) Qualified Entity Certification Program (QECP) (also known as the Medicare Data Sharing for Performance Measurement Program) enables organizations to receive Medicare Parts A and B claims data and Part D prescription drug event data for use in evaluating provider performance.

Organizations approved as Qualified Entities (QEs) are required to use the Medicare data to produce and publicly disseminate CMS-approved reports on provider performance. QEs are also permitted to create non-public analyses and provide or sell such analyses to authorized users. In addition, QEs may provide or sell combined data, or provide Medicare claims data alone at no cost, to certain authorized users.

Under the QECP, CMS certifies QEs to receive these data and monitors certified QEs. As part of the Data Security Review, or Phase 2 of the overall certification process, the organization must complete the following attestation review, titled as the QECP DSR (formerly known as the QECP Data Security Workbook).

The QECP DSR follows a tailored framework modeled after the CMS Acceptable Risk Safeguards (ARS) *Version 3.1*, and provides a roadmap to compliance to ensure that CMS data is adequately secured and appropriately protected.

In addition to completing the QECP DSR, please upload the following context documents into the secure QECP Salesforce Portal:

- An updated Data Flow Diagram with annotations documenting the flow of CMS data within your proposed environment, which includes flow between physical locations and partner environments. An example diagram has been provided in the QECP Phase 2 Toolkit located at https://www.qemedicaredata.org/apex/Phase_2.
- If you are utilizing any vendor(s) (e.g. Cloud Service Provider (CSP), colocation facility, data management vendor), an executed Business Associate Agreement (BAA) between your organization and the vendor(s) that demonstrates an understanding of the nature of data being stored, processed, and transmitted to/from the vendor(s).
- Policy and procedure documents as support for the following five families: Access Control (AC), Identification and Authentication (IA), Media Protection (MP), System and Services Acquisition (SA), System and Information Integrity (SI).

**To complete the QECP DSR, the QE organization must:**

1. Provide organizational details, key contacts, data storage information, and relevant data breach incidents in Sections A, B, C, and D.
2. Complete Section E by attesting to each security/privacy control question by selecting "Yes," "No," or "N/A." Please provide a narrative statement justification in the rationale section for each "No" or "N/A" answer.
3. Complete Section F attesting to the understanding of shared responsibility and completeness of information within the DSR.

**In preparation of completing the QECP DSR, it is recommended that the QE organization:**

- Collaborate with their institutional information security and privacy officials (i.e. the Chief Information Security Officer, Technology Officer, Privacy Officer, System Manager, et al.);
- Collect organizational policies that discuss or mimic ARS security control families (e.g. access control policies, awareness and training policies, audit & accountability policies, etc.); and
- Collect any other organizational policies and/or procedural documents that outline relevant security and privacy baselines.

For any questions on specific controls or protocols when completing the QECP DSR, please contact your organization's assigned QECP Program Manager.

# QECP DSR

## A. QE Organization Information

**Directions:** The Qualified Entity (QE) is the organization that has primary oversight of the research project. The QE may or may not be the entity that stores the identifiable CMS data, but remains responsible for ensuring that controls are in place and operating effectively for all parties, including data custodians and/or collaboration partners.

Please identify the organization(s) participating in the QECP application. Note which physical locations will store the identifiable data, which organizations will access identifiable data, and if remote access to the data will be allowed. *NOTE: CMS will allow only one entity to store identifiable CMS data. This section reflects this requirement by having the data stored **either** with the **QE** or with a **Data Custodian**.

| | | |
|---|---|---|
| QE | <Insert QE Name> | Store Identifiable Data ☐ Yes ☐ No<br>Access Identifiable Data ☐ Yes ☐ No<br>Remote Access ☐ Yes ☐ No |
| Data Custodian | <Insert Data Custodian Name or Not Applicable (N/A)> | Store Identifiable Data ☐ Yes ☐ No<br>Access Identifiable Data ☐ Yes ☐ No<br>Remote Access ☐ Yes ☐ No |
| Collaboration Partner 1 | <Insert Partner Name or Not Applicable (N/A)> | Access Identifiable Data ☐ Yes ☐ No<br>Remote Access ☐ Yes ☐ No |
| Collaboration Partner 1 Address | <Insert Partner Organization Address> | |
| Collaboration Partner 2 | <Insert Partner 2 Name or Not Applicable (N/A)> | Access Identifiable Data ☐ Yes ☐ No<br>Remote Access ☐ Yes ☐ No |
| Collaboration Partner 2 Address | <Insert Partner Organization 2 Address> | |

## B. Key Individuals

**Directions:** Please identify key individuals for the QE organization.

| | | |
|---|---|---|
| Program Owner | <Insert Program Owner Name> | Responsible for overall management and oversight of the program. The main point of contact for the QECP. |
| System Security Officer | <Insert System Security Officer Name and Title> | Individual with overall security responsibility for the data and information systems used in the project. |
| Privacy Officer | <Insert Privacy Officer Name and Title> | Individual with overall privacy responsibility for the information used in the project. |

## C. Data Storage Location(s)

**Directions:** The following section refers to the physical locations under direct control of the QE or Data Custodian where identifiable CMS data will be stored, processed, or accessed. It also includes the name(s) of the individual(s) responsible for each site's **physical security**. *Consider Data Centers, Work Sites, and Offsite Storage Locations (e.g. records management, offsite backup storage).*

| | |
|---|---|
| QE | <Insert QE Name> |
| QE Address | <Insert QE Address> |
| QE Physical Security Contact(s) | <Insert QE Physical Security Contact Name(s)> |
| Data Custodian | <Insert Data Custodian Name> |
| Data Custodian Address | <Insert Data Custodian Address> |
| Data Custodian Physical Security Contact(s) | <Insert Data Custodian Physical Security Contact Name(s)> |
| If Utilizing a Cloud Service Provider (CSP) | <Insert Name of Product Being Used (e.g. AWS US East, Azure Government, etc.) |

## D. Data Security Breaches

**Directions:** Please report any data security breaches that your organization has experienced during the last 10 years. This would include all data security incidents involving unauthorized access or disclosure of Protected Health Information (PHI) and/or Personally Identifiable Information (PII). Also include any unresolved incidents from previous years. Copy the table if multiple incidents need to be reported.

☐ N/A. Our organization has not experienced any data security breaches during the last 10 years.

**Incident 1**

| | |
|---|---|
| Incident Date | <Insert Date of Incident> |
| Source (Internal or External) | <Insert Internal or External> |
| Name of Organization Where Incident Occurred | <Organization Name> |
| Breached Data Type | <Insert PHI or PII or Both> |
| Description of Incident | <Describe Event> |
| Number of Records/Individuals Affected | <Insert Number Affected> |
| Description of Resolution | <Describe Resolution Taken> |
| Resolution Date | <Insert Resolution Date or Pending if in process> |

## E. Security and Privacy Controls

**Directions:** The following security and privacy controls are based on the CMS ARS *Version 3.1*. For each question, please attest to whether or not your organization has implemented the listed control, focusing on the system(s) that will contain CMS data. If "No" or "N/A" is selected, please provide rationale at the end of each sub-section.

### 1. Access Control (AC)

| | | |
|---|---|---|
| AC-1 | Does your organization:<br>a. Have an Access Control policy (and subsequent procedures to facilitate the implementation of that policy) that addresses the purpose, scope, roles, responsibilities, management commitment, | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A |

| | | |
|---|---|---|
| | coordination among organizational entities, and compliance for all parties using CMS data?<br>b. Is that policy and subsequent procedures reviewed and updated (as necessary) at least every 3 years? | |
| AC-2<br>AC-2(2)<br>AC-2(3) | Does your organization's account management system:<br>a. Identify accounts for individuals, applications, groups, systems, guests/anonymous, emergency, and temporary?<br>b. Assign an account manager?<br>c. Establish conditions for group and role membership?<br>d. Ensure unique user accounts?<br>e. Require approvals by defined personnel or roles for account creation?<br>f. Audit records that track account changes (i.e. creating, enabling, modifying, disabling, deleting)?<br>g. Monitor the use of accounts?<br>h. Review user accounts periodically?<br>i. Centralize and automate account management?<br>j. Disable emergency accounts within 24 hours and temporary accounts within 60 days?<br>k. Automatically disable inactive accounts within 60 days? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A<br>c. ☐ Yes ☐ No ☐ N/A<br>d. ☐ Yes ☐ No ☐ N/A<br>e. ☐ Yes ☐ No ☐ N/A<br>f. ☐ Yes ☐ No ☐ N/A<br>g. ☐ Yes ☐ No ☐ N/A<br>h. ☐ Yes ☐ No ☐ N/A<br>i. ☐ Yes ☐ No ☐ N/A<br>j. ☐ Yes ☐ No ☐ N/A<br>k. ☐ Yes ☐ No ☐ N/A |
| AC-3 | Does your organization ensure the information system uses logical access controls to restrict access to information (e.g. roles, groups, file permissions)? | ☐ Yes ☐ No ☐ N/A |
| AC-5 | Does your organization ensure the information system separates the duties of users? | ☐ Yes ☐ No ☐ N/A |
| AC-6<br>AC-6(1)<br>AC-6(2)<br>AC-6(5)<br>AC-6(9)<br>AC-6(10) | Does your organization ensure that users have the fewest permissions required to perform their job functions, to include:<br>a. Disabling non-essential functions and removable media devices?<br>b. Ensuring security functions are explicitly authorized?<br>c. Ensuring that users utilize their own account to access systems, then escalate privileges to perform administrative functions?<br>d. Auditing of all privileged account usage activities? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A<br>c. ☐ Yes ☐ No ☐ N/A<br>d. ☐ Yes ☐ No ☐ N/A |
| AC-7 | Does your organization ensure that the information system enforces the automatic disabling/locking of accounts for 1 hour after 5 invalid login attempts during a 120 minute time window? | ☐ Yes ☐ No ☐ N/A |
| AC-8 | Does your organization ensure that the information system displays a notification or banner that provides appropriate privacy and security notices before gaining access to the system? | ☐ Yes ☐ No ☐ N/A |
| AC-11<br>AC-11(1) | Does your organization: | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A |

| | | |
|---|---|---|
| | a. Ensure that user sessions lock after 15 minutes of inactivity and/or are automatically disconnected under specified circumstances?<br>b. Ensure that the information system conceals, via the session lock, information previously visible on the display with a publicly viewable image? | |
| AC-12 | Does your organization ensure that the information system automatically terminates a user session after defined conditions or trigger events are met? | ☐ Yes ☐ No ☐ N/A |
| AC-14 | Does your organization ensure that the information system defines what actions can be taken on the system without authentication (e.g. viewing certain webpages with public information)? | ☐ Yes ☐ No ☐ N/A |
| AC-17<br>AC-17(1)<br>AC-17(2)<br>AC-17(3) | Does your organization ensure that remote connections:<br>a. Control access to privileged functions?<br>b. Have automated monitoring enabled in order to detect unauthorized connections or cyber-attacks?<br>c. Have connection requirements, such as cryptography, to ensure confidentiality and integrity?<br>d. Are routed through a limited number of managed access control points? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A<br>c. ☐ Yes ☐ No ☐ N/A<br>d. ☐ Yes ☐ No ☐ N/A |
| AC-18<br>AC-18(1) | Does your organization ensure that the information system has usage restrictions and implementation guidance (e.g. encryption, access points in secure areas) **for wireless access**, if that type of access is authorized? | ☐ Yes ☐ No ☐ N/A |
| AC-19<br>AC-19(5) | Does your organization ensure that the information system has usage restrictions and implementation guidance (e.g. appropriate configuration, device identification, updating operating system and antivirus software, full device encryption, etc.) **for mobile devices**, if access by that means is authorized? | ☐ Yes ☐ No ☐ N/A |
| AC-20<br>AC-20(1)<br>AC-20(2) | Does your organization:<br>a. Ensure that the information system does not use systems outside of the authorization boundary to store, transmit, or view system information?<br>b. Permit authorized individuals to use an external information system to access internal systems?<br>c. Restrict the use of organization-controlled portable storage devices by authorized individuals on external information systems? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A<br>c. ☐ Yes ☐ No ☐ N/A |
| AC-21 | Does your organization ensure that the information system has a process for determining what is shared with external users? | ☐ Yes ☐ No ☐ N/A |
| AC-22 | Does your organization properly designate and train authorized individuals to ensure that publicly accessible posted information does not contain nonpublic information? | ☐ Yes ☐ No ☐ N/A |

| | | |
|---|---|---|
| **If "No" or "N/A" was selected for any of the above listed control-specific questions, please provide a brief rationale explaining why your organization has chosen not to implement the applicable control. Please add rows as needed.** | | |
| *Control(s) Referenced* | *Rationale* | *Confirm Box Selected* |
| AC-? | Click or tap here to enter text. | ☐ No ☐ N/A |
| AC-? | Click or tap here to enter text. | ☐ No ☐ N/A |
| **As support for the answers above, please upload specific organizational policy and/or procedural document(s) to the secure QECP Salesforce Portal. In addition, please specify the control(s) referenced, document title, page/section reference, and last reviewed date to support future requests for evidence if required. Please add rows as needed.** | | |
| *Control(s) Referenced* | *Document Title, Page/Section Reference* | *Last Reviewed Date* |
| AC-? | Click or tap here to enter text. | |
| AC-? | Click or tap here to enter text. | |

## 2. Awareness and Training (AT)

| | | |
|---|---|---|
| AT-1 | Does your organization:<br>a. Have an Awareness and Training policy (and subsequent procedures to facilitate the implementation of that policy) that addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance for all parties using CMS data?<br>b. Is that policy and subsequent procedures reviewed and updated (as necessary) at least every 3 years? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A |
| AT-2 | Does your organization ensure that the security training program is administered and completed within 60 days of an individual assuming the role and every 365 days thereafter? | ☐ Yes ☐ No ☐ N/A |
| AT-2(2)<br>AT-3 | Does your organization ensure that the security training program includes modules for security and privacy awareness, insider threat identification, and role-based security? | ☐ Yes ☐ No ☐ N/A |
| AT-4 | Does your organization retain individual security training records for a minimum of 5 years after the individual completes each training? | ☐ Yes ☐ No ☐ N/A |
| **If "No" or "N/A" was selected for any of the above listed control-specific questions, please provide a brief rationale explaining why your organization has chosen not to implement the applicable control. Please add rows as needed.** | | |
| *Control(s) Referenced* | *Rationale* | *Confirm Box Selected* |
| AT-? | Click or tap here to enter text. | ☐ No ☐ N/A |

| | | |
|---|---|---|
| AT-? | Click or tap here to enter text. | ☐ No ☐ N/A |

### 3. Audit and Accountability (AU)

| | | |
|---|---|---|
| AU-1 | Does your organization:<br>a. Have an Audit and Accountability policy (and subsequent procedures to facilitate the implementation of that policy) that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance for all parties using CMS data?<br>b. Is that policy and subsequent procedures reviewed and updated (as necessary) at least every 3 years? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A |
| AU-2 | Does your organization ensure that the information system can audit events, to include:<br>a. Server alerts and error messages?<br>b. User log-on and log-off (successful or unsuccessful)?<br>c. All system administration activities?<br>d. Modification of privileges and access?<br>e. Start up and shut down?<br>f. Application modifications?<br>g. Application alerts and error messages?<br>h. Configuration changes?<br>i. Account creation, modification, or deletion?<br>j. File creation and deletion?<br>k. Read access to sensitive information?<br>l. Modification to sensitive information?<br>m. Printing sensitive information?<br>n. Anomalous (i.e. non-attributable) activity?<br>o. Data as required for privacy monitoring privacy controls?<br>p. Concurrent log on from different work stations?<br>q. Override of access control mechanisms?<br>r. Process creation?<br>s. Attempts to create, read, write, modify, or delete files containing PII? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A<br>c. ☐ Yes ☐ No ☐ N/A<br>d. ☐ Yes ☐ No ☐ N/A<br>e. ☐ Yes ☐ No ☐ N/A<br>f. ☐ Yes ☐ No ☐ N/A<br>g. ☐ Yes ☐ No ☐ N/A<br>h. ☐ Yes ☐ No ☐ N/A<br>i. ☐ Yes ☐ No ☐ N/A<br>j. ☐ Yes ☐ No ☐ N/A<br>k. ☐ Yes ☐ No ☐ N/A<br>l. ☐ Yes ☐ No ☐ N/A<br>m. ☐ Yes ☐ No ☐ N/A<br>n. ☐ Yes ☐ No ☐ N/A<br>o. ☐ Yes ☐ No ☐ N/A<br>p. ☐ Yes ☐ No ☐ N/A<br>q. ☐ Yes ☐ No ☐ N/A<br>r. ☐ Yes ☐ No ☐ N/A<br>s. ☐ Yes ☐ No ☐ N/A |
| AU-2(3) | Does your organization review and updates the list of auditable events at least every 365 days or when a significant change to the system occurs? | ☐ Yes ☐ No ☐ N/A |
| AU-4 | Does your organization ensure adequate storage capacity for 90 days of audit records? | ☐ Yes ☐ No ☐ N/A |
| AU-5 | Does your organization:<br>a. Ensure the information system notifies administrators of audit process failures?<br>b. Take appropriate actions in response to an audit failure or audit storage capacity issue? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A |
| AU-6 | Does your organization: | a. ☐ Yes ☐ No ☐ N/A |

| | | |
|---|---|---|
| AU-6(1)<br>AU-6(3) | a. Ensure that audit records are reviewed weekly for indications of inappropriate or unusual activity?<br>b. Reports findings to defined personnel or roles?<br>c. Review key events (logons, errors, intrusion detection, network traffic, etc.) at least every 24 hours?<br>d. Perform manual reviews of system audit records randomly on demand but no less often than once every 30 days?<br>e. Employ automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities?<br>f. Analyze and correlate audit records across different repositories to gain organization-wide situational awareness?<br>g. Ensure that audit records are searchable? | b. ☐ Yes ☐ No ☐ N/A<br>c. ☐ Yes ☐ No ☐ N/A<br>d. ☐ Yes ☐ No ☐ N/A<br>e. ☐ Yes ☐ No ☐ N/A<br>f. ☐ Yes ☐ No ☐ N/A<br>g. ☐ Yes ☐ No ☐ N/A |
| AU-8<br>AU-8(1) | Does your organization:<br>a. Ensure the internal system clocks generate time stamps for audit records?<br>b. Records time stamps for audit records that can be mapped to UTC or Greenwich Mean Time (GMT)?<br>c. Synchronize the internal information system clocks to an authoritative source, such as NIST Internet Time Servers, when the time difference is greater than 100 milliseconds? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A<br>c. ☐ Yes ☐ No ☐ N/A |
| AU-9<br>AU-9(4) | Does your organization:<br>a. Ensure the audit records and tools are protected from unauthorized access, modification, and deletion?<br>b. Authorize access to management of audit functionality only to those individuals or roles who are not subject to audit by that system? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A |
| AU-11 | Does your organization ensure that audit records are retained for 90 days in "hot" storage and archive storage for 1 year (regular data) or 3 years (PII/PHI data)? | ☐ Yes ☐ No ☐ N/A |

**If "No" or "N/A" was selected for any of the above listed control-specific questions, please provide a brief rationale explaining why your organization has chosen not to implement the applicable control. Please add rows as needed.**

| *Control(s) Referenced* | *Rationale* | *Confirm Box Selected* |
|---|---|---|
| AU-? | Click or tap here to enter text. | ☐ No ☐ N/A |
| AU-? | Click or tap here to enter text. | ☐ No ☐ N/A |

## 4. Security Assessment and Authorization (CA)

| | | |
|---|---|---|
| CA-1 | Does your organization:<br>a. Have a Security Assessment and Authorization policy (and subsequent procedures to facilitate the implementation of that policy) that addresses purpose, scope, roles, responsibilities, | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A |

| | | |
|---|---|---|
| | management commitment, coordination among organizational entities, and compliance for all parties using CMS data?<br>b. Is that policy and subsequent procedures reviewed and updated (as necessary) at least every 3 years? | |
| CA-2<br>CA-2(1) | Does your organization:<br>a. Develop an information security and privacy control assessment plan that describes the scope of the assessment and contains the security and privacy controls under assessment, assessment procedures to determine control effectiveness, the assessment environment/team/roles and responsibilities?<br>b. Conducts the security and privacy controls assessment within every 365 days?<br>c. Produces an assessment report that documents the results of the assessment?<br>d. Provides the written results of the assessment within 30 days after its completion to the Business Owner responsible for the system to facilitate review and necessary system documentation changes?<br>e. Employ independent assessors or assessment teams to conduct the security control assessments? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A<br>c. ☐ Yes ☐ No ☐ N/A<br>d. ☐ Yes ☐ No ☐ N/A<br>e. ☐ Yes ☐ No ☐ N/A |
| CA-3<br>CA-3(5) | Does your organization ensure that external and internal interconnections have:<br>a. An Interconnection Security Agreement (ISA), or other comparable agreement such as MOU/MOA, SLA?<br>b. Documented interfaces, security requirements, and types of information exchanged?<br>c. ISAs updated once per year or after a significant changes?<br>d. A deny-all, permit-by-exception policy for all defined connections? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A<br>c. ☐ Yes ☐ No ☐ N/A<br>d. ☐ Yes ☐ No ☐ N/A |
| CA-5 | Does your organization develop a Plan of Action and Milestones (POAM) within 30 days of the submission of final results for every internal/external audit/review or test in order to facilitate addressing findings and validating completion of related tasks? | ☐ Yes ☐ No ☐ N/A |
| CA-6 | Does your organization have an Authorizing Official (AO) that authorizes the information system for processing prior to commencing any operations within every 3 years or after a significant change occurs? | ☐ Yes ☐ No ☐ N/A |
| CA-7 | Does your organization ensure the information system has a continuous monitoring program to evaluate:<br>a. Metrics related to identified vulnerabilities and remediation?<br>b. Ongoing security assessments? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A |
| CA-8 | Does your organization conduct both internal and external penetration testing, within every 365 days, on identified systems? | ☐ Yes ☐ No ☐ N/A |

| | | |
|---|---|---|
| CA-9 | Does your organization authorize and document connections of defined internal systems, including the types of personally owned equipment that may be internally connected, with organizational systems? | ☐ Yes ☐ No ☐ N/A |

**If "No" or "N/A" was selected for any of the above listed control-specific questions, please provide a brief rationale explaining why your organization has chosen not to implement the applicable control. Please add rows as needed.**

| *Control(s) Referenced* | *Rationale* | *Confirm Box Selected* |
|---|---|---|
| CA-? | Click or tap here to enter text. | ☐ No ☐ N/A |
| CA-? | Click or tap here to enter text. | ☐ No ☐ N/A |

## 5. Configuration Management (CM)

| | | |
|---|---|---|
| CM-1 | Does your organization:<br>a. Have a Configuration Management policy (and subsequent procedures to facilitate the implementation of that policy) that addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance for all parties using CMS data?<br>b. Is that policy and subsequent procedures reviewed and updated (as necessary) at least every 3 years? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A |
| CM-2 | Does your organization ensure that the information system has a current baseline configuration image for hosts within the system? | ☐ Yes ☐ No ☐ N/A |
| CM-2(1) | Does your organization ensure the baseline configuration is reviewed and updated every 365 days or when a critical security patch is necessary? | ☐ Yes ☐ No ☐ N/A |
| CM-3<br>CM-3(2) | Does your organization:<br>a. Define which changes to the system are controlled (i.e. require approval)?<br>b. Review proposed changes with explicit attention to impact on security?<br>c. Document and retain change control decisions for 3 years after the change?<br>d. Periodically audit change control decisions?<br>e. Test, validate, and document changes to the information system before implementing the changes on the operational system? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A<br>c. ☐ Yes ☐ No ☐ N/A<br>d. ☐ Yes ☐ No ☐ N/A<br>e. ☐ Yes ☐ No ☐ N/A |
| CM-4 | Does your organization:<br>a. Analyze changes to the information system to determine potential security and privacy impacts prior to change implementation?<br>b. Audit activities associated with configuration changes? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A |

| | | |
|---|---|---|
| CM-5 | Does your organization ensure that the information system uses physical and logical access restrictions to prevent unauthorized changes to the system? | ☐ Yes ☐ No ☐ N/A |
| CM-7<br>CM-7(1)<br>CM-7(2)<br>CM-7(5) | Does your organization:<br>a. Ensure that the information system only allows essential capabilities, functions, software, ports, network protocols, and applications?<br>b. Review the information system no less often than once every 30 days to identify and eliminate unnecessary functions, ports, protocols, and/or services?<br>c. Perform automated reviews of the system no less often than once every 72 hours to identify changes in functions, ports, protocols, and/or services?<br>d. Disable functions, ports, protocols, and services within the system deemed to be unnecessary and/or non-secure?<br>e. Prevent program execution for unauthorized software?<br>f. Identifies defined software programs authorized to execute (whitelist) on the information system and reviews and updates that list every 72 hours? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A<br>c. ☐ Yes ☐ No ☐ N/A<br>d. ☐ Yes ☐ No ☐ N/A<br>e. ☐ Yes ☐ No ☐ N/A<br>f. ☐ Yes ☐ No ☐ N/A |
| CM-8 | Does your organization ensure that the information system maintains an up-to-date system inventory of all system components, including:<br>a. Each component's unique identifier and/or serial number?<br>b. Information system of which the component is a part<br>c. Type of information system component (e.g. server, desktop, application)?<br>d. Manufacturer/model information?<br>e. Operating system type and version/service pack level?<br>f. Presence of virtual machines?<br>g. Application software version/license information?<br>h. Physical location (e.g. building/room number)?<br>i. Logical location (e.g. IP address, position with the information system [IS] architecture)?<br>j. Media access control (MAC) address?<br>k. Ownership?<br>l. Operational status?<br>m. Primary and secondary administrators?<br>n. Primary user? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A<br>c. ☐ Yes ☐ No ☐ N/A<br>d. ☐ Yes ☐ No ☐ N/A<br>e. ☐ Yes ☐ No ☐ N/A<br>f. ☐ Yes ☐ No ☐ N/A<br>g. ☐ Yes ☐ No ☐ N/A<br>h. ☐ Yes ☐ No ☐ N/A<br>i. ☐ Yes ☐ No ☐ N/A<br>j. ☐ Yes ☐ No ☐ N/A<br>k. ☐ Yes ☐ No ☐ N/A<br>l. ☐ Yes ☐ No ☐ N/A<br>m. ☐ Yes ☐ No ☐ N/A<br>n. ☐ Yes ☐ No ☐ N/A |
| CM-8(1) | Does your organization update the inventory of information system components as an integral part of component installations, removals, and information system updates? | ☐ Yes ☐ No ☐ N/A |
| CM-11 | Does your organization ensure that the information system prevents users from installing software through user policies? | ☐ Yes ☐ No ☐ N/A |

**If "No" or "N/A" was selected for any of the above listed control-specific questions, please provide a brief rationale explaining why your organization has chosen not to implement the applicable control. Please add rows as needed.**

| *Control(s) Referenced* | *Rationale* | *Confirm Box Selected* |
|---|---|---|
| CM-? | Click or tap here to enter text. | ☐ No ☐ N/A |
| CM-? | Click or tap here to enter text. | ☐ No ☐ N/A |

## 6. Contingency Planning (CP)

| | | |
|---|---|---|
| CP-1 | Does your organization:<br>a. Have a Contingency Planning policy (and subsequent procedures to facilitate the implementation of that policy) that addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance for all parties using CMS data?<br>b. Is that policy and subsequent procedures reviewed and updated (as necessary) at least every 3 years? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A |

**If "No" or "N/A" was selected for any of the above listed control-specific questions, please provide a brief rationale explaining why your organization has chosen not to implement the applicable control. Please add rows as needed.**

| *Control(s) Referenced* | *Rationale* | *Confirm Box Selected* |
|---|---|---|
| CP-1 | Click or tap here to enter text. | ☐ No ☐ N/A |

## 7. Identification and Authentication (IA)

| | | |
|---|---|---|
| IA-1 | Does your organization:<br>a. Have an Identification and Authentication policy (and subsequent procedures to facilitate the implementation of that policy) that addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance for all parties using CMS data?<br>b. Is that policy and subsequent procedures reviewed and updated (as necessary) at least every 3 years? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A |
| IA-2<br>IA-2(1)<br>IA-2(2)<br>IA-2(3)<br>IA-2(8) | Does your organization:<br>a. Ensure that the information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users?<br>b. Implement multifactor authentication (MFA) for network access to privileged accounts?<br>c. Implement MFA for network access to non-privileged accounts?<br>d. Implement MFA for local access to privileged accounts?<br>e. Implement replay-resistant authentication mechanisms for network access to privileged accounts? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A<br>c. ☐ Yes ☐ No ☐ N/A<br>d. ☐ Yes ☐ No ☐ N/A<br>e. ☐ Yes ☐ No ☐ N/A |

| | | |
|---|---|---|
| IA-3 | Does your organization ensure that the information system uniquely identifies devices (e.g. IP address, hostname)? | ☐ Yes ☐ No ☐ N/A |
| IA-4 | Does your organization ensure that the information system:<br>a. Successfully assigns unique identifiers to users and devices?<br>b. Does not reuse identifiers for 3 years?<br>c. Disables inactive identifiers after 60 days of inactivity? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A<br>c. ☐ Yes ☐ No ☐ N/A |
| IA-5<br>IA-5(1) | Does your organization ensure that the information system:<br>a. Verifies that the correct identifier is being issued to a person or device during authenticator distribution?<br>b. Has a standard for authenticator schema (e.g. first initial, last name, number if duplicate)?<br>c. Prohibits the use of dictionary names or words?<br>d. Meets or exceeds enforcement ARS baseline minimum password requirements?<br>e. Confirms the minimum password length for regular user passwords is 8 characters and 15 characters for administrators or privileged user passwords?<br>f. Sets the value at 6, if the operating environment enforces a minimum of number of changed characters when new passwords are created?<br>g. Stores and transmits only encrypted representations of passwords?<br>h. Allows the use of a temporary password for system logons with an immediate change to a permanent password? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A<br>c. ☐ Yes ☐ No ☐ N/A<br>d. ☐ Yes ☐ No ☐ N/A<br>e. ☐ Yes ☐ No ☐ N/A<br>f. ☐ Yes ☐ No ☐ N/A<br>g. ☐ Yes ☐ No ☐ N/A<br>h. ☐ Yes ☐ No ☐ N/A |
| IA-6 | Does your organization ensure that the system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals? | ☐ Yes ☐ No ☐ N/A |
| IA-8 | Does your organization ensure that the system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users) prior to gaining access to all systems and networks? | ☐ Yes ☐ No ☐ N/A |

**If "No" or "N/A" was selected for any of the above listed control-specific questions, please provide a brief rationale explaining why your organization has chosen not to implement the applicable control. Please add rows as needed.**

| *Control(s) Referenced* | *Rationale* | *Confirm Box Selected* |
|---|---|---|
| IA-? | Click or tap here to enter text. | ☐ No ☐ N/A |
| IA-? | Click or tap here to enter text. | ☐ No ☐ N/A |

| **As support for the answers above, please upload specific organizational policy and/or procedural document(s) to the secure QECP Salesforce Portal. In addition, please specify the control(s) referenced, document title, page/section reference, and last reviewed date to support future requests for evidence if required. Please add rows as needed.** | | |
|---|---|---|
| *Control(s) Referenced* | *Document Title, Page/Section Reference* | *Last Reviewed Date* |
| IA-? | Click or tap here to enter text. | |
| IA-? | Click or tap here to enter text. | |

## 8. Incident Response (IR)

| | | |
|---|---|---|
| IR-1 | Does your organization:<br>a. Have an Incident Response policy (and subsequent procedures to facilitate the implementation of that policy) that addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance for all parties using CMS data?<br>b. Is that policy and subsequent procedures reviewed and updated (as necessary) at least every 3 years? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A |
| IR-2 | Does your organization ensure that employees whom have incident response duties complete incident response training within 1 month of assuming the role and complete an incident response training every 365 days thereafter? | ☐ Yes ☐ No ☐ N/A |
| IR-3 | Does your organization test the incident response capability of the information system within every 365 days to determine the organization's incident response effectiveness, and documents its findings? | ☐ Yes ☐ No ☐ N/A |
| IR-4 | Does your organization:<br>a. Implement an incident handling capability?<br>b. Coordinate incident handling activities with contingency planning activities?<br>c. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A<br>c. ☐ Yes ☐ No ☐ N/A |
| IR-5 | Does your organization track and document all physical, information security, and privacy incidents? | ☐ Yes ☐ No ☐ N/A |
| IR-6 | Does your organization require personnel to report actual or suspected security and privacy incidents? | ☐ Yes ☐ No ☐ N/A |
| IR-7 | Does your organization provide an incident response support resource, integral to the organizational incident response function, who offers advice and assistance to users of the information system for the handling and reporting of security incidents? | ☐ Yes ☐ No ☐ N/A |

| | | |
|---|---|---|
| IR-8 | Does your organization develop an incident response plan that:<br>a. Provides the organization with a roadmap for implementing its incident response capability?<br>b. Describes the structure and organization of the incident response capability?<br>c. Provides a high-level approach for how the incident response capability fits into the overall organization?<br>d. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions?<br>e. Defines reportable incidents?<br>f. Provides metrics for measuring the incident response capability within the organization?<br>g. Defines the resources and management support needed to effectively maintain and mature an incident response capability?<br>h. Is reviewed and approved by the applicable Incident Response Team Leader?<br>i. Is distributed via copies to necessary CMS information security officers and other incident response team personnel?<br>j. Is reviewed within every 365 days?<br>k. Is updated to address system/organizational changes or problems encountered during plan implementation, execution, or testing?<br>l. Communicates incident response plan changes to the appropriate CMS and organizational parties?<br>m. Is protected from unauthorized disclosure and modification? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A<br>c. ☐ Yes ☐ No ☐ N/A<br>d. ☐ Yes ☐ No ☐ N/A<br>e. ☐ Yes ☐ No ☐ N/A<br>f. ☐ Yes ☐ No ☐ N/A<br>g. ☐ Yes ☐ No ☐ N/A<br>h. ☐ Yes ☐ No ☐ N/A<br>i. ☐ Yes ☐ No ☐ N/A<br>j. ☐ Yes ☐ No ☐ N/A<br>k. ☐ Yes ☐ No ☐ N/A<br>l. ☐ Yes ☐ No ☐ N/A<br>m. ☐ Yes ☐ No ☐ N/A |

**If "No" or "N/A" was selected for any of the above listed control-specific questions, please provide a brief rationale explaining why your organization has chosen not to implement the applicable control. Please add rows as needed.**

| *Control(s) Referenced* | *Rationale* | *Confirm Box Selected* |
|---|---|---|
| IR-? | Click or tap here to enter text. | ☐ No ☐ N/A |
| IR-? | Click or tap here to enter text. | ☐ No ☐ N/A |

## 9. Maintenance (MA)

| | | |
|---|---|---|
| MA-1 | Does your organization:<br>a. Have a Maintenance policy (and subsequent procedures to facilitate the implementation of that policy) that addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance for all parties using CMS data?<br>b. Is that policy and subsequent procedures reviewed and updated (as necessary) at least every 3 years? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A |
| MA-2 | Does your organization: | a. ☐ Yes ☐ No ☐ N/A |

| | | |
|---|---|---|
| | a. Schedule, perform, document, and review records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements?<br>b. Approve and monitor all maintenance activities, whether performed on-site or remotely?<br>c. Require that applicable staff approve the removal of system or system components from the organizational facilities for off-site maintenance or repairs?<br>d. Sanitize equipment to remove all information from associated media prior to removal?<br>e. Check all potentially impacted security controls to verify that controls are still functioning following maintenance or repair actions?<br>f. Include defined maintenance-related information in organizational maintenance records? | b. ☐ Yes ☐ No ☐ N/A<br>c. ☐ Yes ☐ No ☐ N/A<br>d. ☐ Yes ☐ No ☐ N/A<br>e. ☐ Yes ☐ No ☐ N/A<br>f. ☐ Yes ☐ No ☐ N/A |
| MA-3<br>MA-3(1)<br>MA-3(2) | Does your organization:<br>a. Approve, control, and monitor information system maintenance tools?<br>b. Inspect the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications?<br>c. Check media containing diagnostic and test programs for malicious code before the media are used in the information system? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A<br>c. ☐ Yes ☐ No ☐ N/A |
| MA-4 | Does your organization:<br>a. Allow the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy?<br>b. Employ strong identification and authentication techniques in the establishment of nonlocal maintenance and diagnostic sessions?<br>c. Maintain records for nonlocal maintenance and diagnostic activities?<br>d. Terminate all sessions and network connections when nonlocal maintenance is completed? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A<br>c. ☐ Yes ☐ No ☐ N/A<br>d. ☐ Yes ☐ No ☐ N/A |
| MA-5 | Does your organization:<br>a. Establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel?<br>b. Ensure that non-escorted personnel performing maintenance on the information system have required access authorizations?<br>c. Designate organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A<br>c. ☐ Yes ☐ No ☐ N/A |

| **If "No" or "N/A" was selected for any of the above listed control-specific questions, please provide a brief rationale explaining why your organization has chosen not to implement the applicable control. Please add rows as needed.** | | |
|---|---|---|
| *Control(s) Referenced* | *Rationale* | *Confirm Box Selected* |
| MA-? | Click or tap here to enter text. | ☐ No ☐ N/A |
| MA-? | Click or tap here to enter text. | ☐ No ☐ N/A |

## 10. Media Protection (MP)

| | | |
|---|---|---|
| MP-1 | Does your organization:<br>a. Have a Media Protection policy (and subsequent procedures to facilitate the implementation of that policy) that addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance for all parties using CMS data?<br>b. Is that policy and subsequent procedures reviewed and updated (as necessary) at least every 3 years? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A |
| MP-2 | Does your organization restrict access to sensitive digital and non-digital media by disabling CD/DVD writers and USB ports to only allow access for appropriate personnel? | ☐ Yes ☐ No ☐ N/A |
| MP-3 | Does your organization ensure that the information system marks system media based on the classification of information the media holds? | ☐ Yes ☐ No ☐ N/A |
| MP-4 | Does your organization:<br>a. Physically control and securely store digital and non-digital media within controlled areas?<br>b. Protect information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures. | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A |
| MP-5<br>MP-5(4) | Does your organization ensure that the information system protects media while being transported, to include:<br>a. Hand-carried – Uses a securable container (e.g. locked briefcase) via authorized personnel?<br>b. Shipping – Tracks with receipt by commercial carrier?<br>c. Maintaining accountability for information system media during transport outside of controlled areas?<br>d. Documenting activities associated with the transport of information system media?<br>e. Restricting the activities associated with the transport of information system media to authorized personnel? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A<br>c. ☐ Yes ☐ No ☐ N/A<br>d. ☐ Yes ☐ No ☐ N/A<br>e. ☐ Yes ☐ No ☐ N/A<br>f. ☐ Yes ☐ No ☐ N/A |

| | | |
|---|---|---|
| | f. Implementing cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas? | |
| MP-6<br>MP-6(1) | Does your organization:<br>a. Sanitize both digital and non-digital media prior to disposal, release out of organizational control, or release for reuse using defined sanitization techniques and procedures?<br>b. Review, approve, track, document, and verify media sanitization and disposal actions? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A |
| MP-7<br>MP-7(1) | Does your organization:<br>a. Ensure that the information system prohibits the use of personally owned media?<br>b. Prohibits the use of portable storage devices that have no identifiable owner? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A |
| MP-CMS-1 | Does your organization ensure that records of disposed media which contain sensitive information are maintained? | ☐ Yes ☐ No ☐ N/A |

**If "No" or "N/A" was selected for any of the above listed control-specific questions, please provide a brief rationale explaining why your organization has chosen not to implement the applicable control. Please add rows as needed.**

| *Control(s) Referenced* | *Rationale* | *Confirm Box Selected* |
|---|---|---|
| MP-? | Click or tap here to enter text. | ☐ No ☐ N/A |
| MP-? | Click or tap here to enter text. | ☐ No ☐ N/A |

**As support for the answers above, please upload specific organizational policy and/or procedural document(s) to the secure QECP Salesforce Portal. In addition, please specify the control(s) referenced, document title, page/section reference, and last reviewed date to support future requests for evidence if required. Please add rows as needed.**

| *Control(s) Referenced* | *Document Title, Page/Section Reference* | *Last Reviewed Date* |
|---|---|---|
| MP-? | Click or tap here to enter text. | |
| MP-? | Click or tap here to enter text. | |

## 11. Physical and Environmental Protection (PE)

| | | |
|---|---|---|
| PE-1 | Does your organization:<br>a. Have a Physical and Environmental Protection policy (and subsequent procedures to facilitate the implementation of that policy) that addresses the purpose, scope, roles, responsibilities, | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A |

| | | |
|---|---|---|
| | management commitment, coordination among organizational entities, and compliance for all parties using CMS data?<br>b. Is that policy and subsequent procedures reviewed and updated (as necessary) at least every 3 years? | |
| PE-2 | Does your organization:<br>a. Ensure that the information system maintains a current list of authorized individuals to enter the facility?<br>b. Issue authorization credentials for facility access?<br>c. Review the access list detailing authorized facility access by individuals every 180 days?<br>d. Remove individuals from facility access list when access is no longer required? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A<br>c. ☐ Yes ☐ No ☐ N/A<br>d. ☐ Yes ☐ No ☐ N/A |
| PE-3 | Does your organization:<br>a. Verify individual access authorizations before granting access to the facility?<br>b. Control ingress/egress to the facility using guards and/or defined physical access control systems/devices (defined in the applicable security plan)?<br>c. Maintain physical access audit logs for defined entry/exit points (defined in the applicable security plan)?<br>d. Provide defined security safeguards (defined in the applicable security plan) to control access to areas within the facility officially designated as publicly accessible?<br>e. Escort visitors and monitors visitor activity in defined circumstances requiring visitor escorts and monitoring (defined in the applicable security plan)?<br>f. Secure keys, combinations, and other physical access devices?<br>g. Inventory define physical access devices (defined in the applicable security plan), no less often than every 90 days?<br>h. Change combinations and keys for defined high-risk entry/exit points (defined in the applicable security plan) within every 365 days, and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A<br>c. ☐ Yes ☐ No ☐ N/A<br>d. ☐ Yes ☐ No ☐ N/A<br>e. ☐ Yes ☐ No ☐ N/A<br>f. ☐ Yes ☐ No ☐ N/A<br>g. ☐ Yes ☐ No ☐ N/A<br>h. ☐ Yes ☐ No ☐ N/A |
| PE-4 | Does your organization ensure that telephone and network hardware and transmission lines (e.g. wiring closets, patch panels, etc.) are protected? | ☐ Yes ☐ No ☐ N/A |
| PE-5 | Does your organization control physical access to output devices (printers, etc.)? | ☐ Yes ☐ No ☐ N/A |
| PE-6 | Does your organization:<br>a. Monitor physical access to the facility where CMS data resides and respond to physical security incidents?<br>b. Review physical access logs weekly and upon occurrence of security incidents?<br>c. Coordinate results of reviews and investigations with the organization's incident response capability? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A<br>c. ☐ Yes ☐ No ☐ N/A |
| PE-8 | Does your organization:<br>a. Maintain visitor access records to the facility for 2 years?<br>b. Review visitor access records no less often than monthly? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A |

| **If "No" or "N/A" was selected for any of the above listed control-specific questions, please provide a brief rationale explaining why your organization has chosen not to implement the applicable control. Please add rows as needed.** | | |
|---|---|---|
| *Control(s) Referenced* | *Rationale* | *Confirm Box Selected* |
| PE-? | Click or tap here to enter text. | ☐ No ☐ N/A |
| PE-? | Click or tap here to enter text. | ☐ No ☐ N/A |

## 12. Planning (PL)

| | | |
|---|---|---|
| PL-1 | Does your organization:<br>a. Have a Planning policy (and subsequent procedures to facilitate the implementation of that policy) that addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance for all parties using CMS data?<br>b. Is that policy and subsequent procedures reviewed and updated (as necessary) at least every 3 years? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A |
| PL-2 | Does your organization:<br>a. Develop comprehensive security plans for information systems?<br>b. Distribute copies of the plans and communicate changes to appropriate personnel?<br>c. Review the security plans every 365 days?<br>d. Update the plans at a minimum every 3 years?<br>e. Protect the security plans from unauthorized disclosure and modification? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A<br>c. ☐ Yes ☐ No ☐ N/A<br>d. ☐ Yes ☐ No ☐ N/A<br>e. ☐ Yes ☐ No ☐ N/A |
| PL-4<br>PL-4(1) | Does your organization:<br>a. Establish and make readily available to individuals requiring access to systems, the rules that describe their responsibilities and expected behavior regarding usage?<br>b. Receive an acknowledgement from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before accessing the system?<br>c. Review and update the rules of behavior every 3 years?<br>d. Require individuals who have previously acknowledged rules of behavior to read and re-acknowledge when rules are revised/updated and at least every 365 days?<br>e. Inform employees and contractors that misuse of CMS data is a violation and is grounds for disciplinary action, monetary fines, and/or criminal charges that could result in imprisonment?<br>f. Include in the rules of behavior, explicit restrictions on the use of social media/networking sites and posting organizational information on public websites? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A<br>c. ☐ Yes ☐ No ☐ N/A<br>d. ☐ Yes ☐ No ☐ N/A<br>e. ☐ Yes ☐ No ☐ N/A<br>f. ☐ Yes ☐ No ☐ N/A |
| **If "No" or "N/A" was selected for any of the above listed control-specific questions, please provide a brief rationale explaining why your organization has chosen not to implement the applicable control. Please add rows as needed.** | | |

| *Control(s) Referenced* | *Rationale* | *Confirm Box Selected* |
|---|---|---|
| PL-? | Click or tap here to enter text. | ☐ No ☐ N/A |
| PL-? | Click or tap here to enter text. | ☐ No ☐ N/A |

**13. Personnel Security (PS)**

| | | |
|---|---|---|
| PS-1 | Does your organization:<br>a. Have a Personnel Security policy (and subsequent procedures to facilitate the implementation of that policy) that addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance for all parties using CMS data?<br>b. Is that policy and subsequent procedures reviewed and updated (as necessary) at least every 3 years? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A |
| PS-3 | Does your organization:<br>a. Screen individuals prior to authorizing access to the information system?<br>b. Rescreen individuals periodically and anytime they move to a new position with a higher risk designation?<br>c. Conduct background investigations?<br>d. Perform reinvestigations for active national security clearances?<br>e. Refuse employees and contractors access to the system until they have been vetted and sign appropriate access agreements? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A<br>c. ☐ Yes ☐ No ☐ N/A<br>d. ☐ Yes ☐ No ☐ N/A<br>e. ☐ Yes ☐ No ☐ N/A |
| PS-4 | Does your organization ensure that employee termination follows the following steps:<br>a. Disables information system access before or during termination?<br>b. Terminates/revokes any authenticators/credentials associated with the individual?<br>c. Conducts exit interviews that include a discussion of non-disclosure of information security and privacy information?<br>d. Retrieves all security-related organizational information system-related property?<br>e. Retains access to organizational information and information systems formerly controlled by the terminated individual?<br>f. Notifies defined personnel or roles (defined in the applicable security plan) within 1 calendar day?<br>g. Immediately escorts employees terminated for cause out of the organization? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A<br>c. ☐ Yes ☐ No ☐ N/A<br>d. ☐ Yes ☐ No ☐ N/A<br>e. ☐ Yes ☐ No ☐ N/A<br>f. ☐ Yes ☐ No ☐ N/A<br>g. ☐ Yes ☐ No ☐ N/A |
| PS-5 | Does your organization:<br>a. Review and confirm ongoing need for current logical and physical access when individuals are reassigned or transfer to other positions within the organization? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A |

| | | |
|---|---|---|
| | b. Notify security management for modification of access cards and any applicable accounts within 30 days of the reassignment or transfer? | |
| PS-6 | Does your organization:<br>a. Develop and document access agreements?<br>b. Review and update those agreements at a minimum of every 365 days?<br>c. Ensure that individuals requiring access acknowledge those agreements prior to access and re-acknowledge within 365 days when those agreements have been updated? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A<br>c. ☐ Yes ☐ No ☐ N/A |
| PS-7 | Does your organization ensure that third-party service providers (contractors, CSPs, vendor maintenance) follow the same personnel requirements as full-time employees? | ☐ Yes ☐ No ☐ N/A |

**If "No" or "N/A" was selected for any of the above listed control-specific questions, please provide a brief rationale explaining why your organization has chosen not to implement the applicable control. Please add rows as needed.**

| *Control(s) Referenced* | *Rationale* | *Confirm Box Selected* |
|---|---|---|
| PS-? | Click or tap here to enter text. | ☐ No ☐ N/A |
| PS-? | Click or tap here to enter text. | ☐ No ☐ N/A |

## 14. Risk Assessment (RA)

| | | |
|---|---|---|
| RA-1 | Does your organization:<br>a. Have a Risk Assessment policy (and subsequent procedures to facilitate the implementation of that policy) that addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance for all parties using CMS data?<br>b. Is that policy and subsequent procedures reviewed and updated (as necessary) at least every 3 years? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A |
| RA-3 | Does your organization:<br>a. Conduct an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits?<br>b. Document risk assessment results in the applicable security plan?<br>c. Review risk assessment results within every 365 days?<br>d. Disseminate risk assessment results to affected stakeholders and Business Owners?<br>e. Update the risk assessment every 3 years, or whenever there are significant changes to the system? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A<br>c. ☐ Yes ☐ No ☐ N/A<br>d. ☐ Yes ☐ No ☐ N/A<br>e. ☐ Yes ☐ No ☐ N/A |
| RA-5<br>RA-5(5) | Does your organization: | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A |

| | | |
|---|---|---|
| | a. Scan for vulnerabilities in the information system and hosted systems no less often than once every 72 hours and when new vulnerabilities are identified?<br>b. Employ vulnerability scanning tools and techniques?<br>c. Analyze vulnerability scan reports and results?<br>d. Remediate vulnerabilities based on the Business Owner's risk prioritization?<br>e. Share information obtained from vulnerability scans and security control assessments with affected/related stakeholders to facilitate eliminated similar vulnerabilities in other systems?<br>f. Implement privileged access authorization to operating system, telecommunications, and configuration components for selected vulnerability scanning activities to facilitate more thorough scanning? | c. ☐ Yes ☐ No ☐ N/A<br>d. ☐ Yes ☐ No ☐ N/A<br>e. ☐ Yes ☐ No ☐ N/A<br>f. ☐ Yes ☐ No ☐ N/A |

**If "No" or "N/A" was selected for any of the above listed control-specific questions, please provide a brief rationale explaining why your organization has chosen not to implement the applicable control. Please add rows as needed.**

| *Control(s) Referenced* | *Rationale* | *Confirm Box Selected* |
|---|---|---|
| RA-? | Click or tap here to enter text. | ☐ No ☐ N/A |
| RA-? | Click or tap here to enter text. | ☐ No ☐ N/A |

## 15. System and Services Acquisition (SA)

| | | |
|---|---|---|
| SA-1 | Does your organization:<br>a. Have a System and Services Acquisition policy (and subsequent procedures to facilitate the implementation of that policy) that addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance for all parties using CMS data?<br>b. Is that policy and subsequent procedures reviewed and updated (as necessary) at least every 3 years? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A |
| SA-2 | Does your organization:<br>a. Determine information security requirements for the information system or service in mission/business process planning?<br>b. Determine, document, and allocate the resources required to protect the information system or service as part of its capital planning and investment control process?<br>c. Include information security requirements in mission/business case planning?<br>d. Establish a discrete line item for the implementation and management of information systems security? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A<br>c. ☐ Yes ☐ No ☐ N/A<br>d. ☐ Yes ☐ No ☐ N/A |
| SA-4 | Does your organization include the following requirements in the acquisition contract (e.g. executed BAA) for the information system:<br>a. Security functional requirements? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A |

| | | |
|---|---|---|
| | b. Security strength requirements?<br>c. Security assurance requirements?<br>d. Security-related documentation requirements?<br>e. Requirements for protecting security-related documentation?<br>f. Description of the system development environment and environment in which the system is intended to operate?<br>g. Acceptance criteria? | c. ☐ Yes ☐ No ☐ N/A<br>d. ☐ Yes ☐ No ☐ N/A<br>e. ☐ Yes ☐ No ☐ N/A<br>f. ☐ Yes ☐ No ☐ N/A<br>g. ☐ Yes ☐ No ☐ N/A |
| SA-5 | Does your organization:<br>a. Obtain administrator documentation for the system?<br>b. Obtain user documentation for the system?<br>c. Document attempts to obtain documentation that is either unavailable or nonexistent?<br>d. Protect documentation as required?<br>e. Distribute documentation to defined personnel or roles? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A<br>c. ☐ Yes ☐ No ☐ N/A<br>d. ☐ Yes ☐ No ☐ N/A<br>e. ☐ Yes ☐ No ☐ N/A |
| SA-8 | Does your organization ensure that the information system architecture is designed following security engineering principles? | ☐ Yes ☐ No ☐ N/A |
| SA-9 | Does your organization ensure that any external connections outside of the accreditation boundary include an Interconnection Service Agreement or similar agreement? | ☐ Yes ☐ No ☐ N/A |

**If "No" or "N/A" was selected for any of the above listed control-specific questions, please provide a brief rationale explaining why your organization has chosen not to implement the applicable control. Please add rows as needed.**

| *Control(s) Referenced* | *Rationale* | *Confirm Box Selected* |
|---|---|---|
| SA-? | Click or tap here to enter text. | ☐ No ☐ N/A |
| SA-? | Click or tap here to enter text. | ☐ No ☐ N/A |

**As support for the answers above, please upload specific organizational policy and/or procedural document(s) to the secure QECP Salesforce Portal. In addition, please specify the control(s) referenced, document title, page/section reference, and last reviewed date to support future requests for evidence if required. Please add rows as needed.**

| *Control(s) Referenced* | *Document Title, Page/Section Reference* | *Last Reviewed Date* |
|---|---|---|
| SA-? | Click or tap here to enter text. | |
| SA-? | Click or tap here to enter text. | |

## 16. System and Communications Protection (SC)

| | | |
|---|---|---|
| SC-1 | Does your organization:<br>a. Have a System and Communications Protection policy (and subsequent procedures to facilitate the implementation of that policy) that addresses the purpose, scope, roles, responsibilities, | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A |

| | | |
|---|---|---|
| | management commitment, coordination among organizational entities, and compliance for all parties using CMS data?<br>b. Is that policy and subsequent procedures reviewed and updated (as necessary) at least every 3 years? | |
| SC-2 | Does your organization ensure that administrative and regular user interfaces are separate? | ☐ Yes ☐ No ☐ N/A |
| SC-4 | Does your organization prevent unauthorized and unintended information transfer via shared system resources? | ☐ Yes ☐ No ☐ N/A |
| SC-7<br>SC-7(3)<br>SC-7(5)<br>SC-7(7) | Does your organization ensure that the information system:<br>a. Monitors and controls communications at the external boundary, both physically and logically, of the system and at key internal boundaries within the system (e.g. firewall, IDS/IPS)?<br>b. Implements subnetworks for publicly accessible system components that are logically separated from internal organizational networks?<br>c. Connects to external networks or information systems only through managed interfaces in accordance with an organizational security architecture?<br>d. Limits the number of external network connections?<br>e. At managed interfaces denies network communications traffic by default and allows network communications traffic by exception (i.e. deny all, permit by exception)?<br>f. In conjunction with a remote device, prevents the device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A<br>c. ☐ Yes ☐ No ☐ N/A<br>d. ☐ Yes ☐ No ☐ N/A<br>e. ☐ Yes ☐ No ☐ N/A<br>f. ☐ Yes ☐ No ☐ N/A |
| SC-10 | Does your organization ensure that the information system disconnects:<br>a. Dynamic Host Configuration Protocol (DHCP) sessions after 7 days?<br>b. VPN connections after 30 minutes of inactivity?<br>c. Has the ability to terminate a network connection as required? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A<br>c. ☐ Yes ☐ No ☐ N/A |
| SC-12 | Does your organization ensure that the information system has a cryptographic key management system that complies with HHS standards? | ☐ Yes ☐ No ☐ N/A |
| SC-13 | Does your organization ensure that the information system uses FIPS 140-2 validated cryptographic modules for transmission of data in motion and/or at rest? | ☐ Yes ☐ No ☐ N/A |
| SC-15 | Does your organization prohibit running collaborative computing mechanisms (e.g. networked white boards, cameras, and microphones) unless explicitly authorized? | ☐ Yes ☐ No ☐ N/A |
| SC-23 | Does your organization protect the authenticity of communication sessions? | ☐ Yes ☐ No ☐ N/A |
| SC-28 | Does your organization protect the confidentiality and integrity of information (PII and PHI) at rest? | ☐ Yes ☐ No ☐ N/A |

| | | |
|---|---|---|
| SC-CMS-1 | Does your organization implement controls to protect sensitive information that is sent via email? | ☐ Yes ☐ No ☐ N/A |

**If "No" or "N/A" was selected for any of the above listed control-specific questions, please provide a brief rationale explaining why your organization has chosen not to implement the applicable control. Please add rows as needed.**

| *Control(s) Referenced* | *Rationale* | *Confirm Box Selected* |
|---|---|---|
| SC-? | Click or tap here to enter text. | ☐ No ☐ N/A |
| SC-? | Click or tap here to enter text. | ☐ No ☐ N/A |

## 17. System and Information Integrity (SI)

| | | |
|---|---|---|
| SI-1 | Does your organization:<br>a. Have a System and Information Integrity policy (and subsequent procedures to facilitate the implementation of that policy) that addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance for all parties using CMS data?<br>b. Is that policy and subsequent procedures reviewed and updated (as necessary) at least every 3 years? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A |
| SI-2 | Does your organization:<br>a. Identify, report, and correct system flaws?<br>b. Test flaw remediation updates prior to installation on production systems?<br>c. Correct security related system flaws within 10 business days on production servers, 30 days on all others? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A<br>c. ☐ Yes ☐ No ☐ N/A |
| SI-3<br>SI-3(1)<br>SI-3(2) | Does your organization information system use malicious code protection that:<br>a. Is installed at system entry and exit points to detect and eradicate malicious code?<br>b. Scans critical file systems every 12 hours and full system scans no less often than once every 72 hours?<br>c. Is centrally managed?<br>d. Has up-to-date virus definitions? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A<br>c. ☐ Yes ☐ No ☐ N/A<br>d. ☐ Yes ☐ No ☐ N/A |
| SI-4<br>SI-4(4)<br>SI-4(5)<br>SI-4(14) | Does your organization monitor the information system for:<br>a. Attacks and indicators of potential attacks?<br>b. Unauthorized local, network, and remote connections?<br>c. Inbound and outbound communications traffic at a defined frequency for unusual or unauthorized activities or conditions?<br>d. Generated alerts to defined personnel notifying of presence of malicious code, unauthorized export of information, or potential intrusions?<br>e. Rogue wireless devices in order to detect attack attempts? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A<br>c. ☐ Yes ☐ No ☐ N/A<br>d. ☐ Yes ☐ No ☐ N/A<br>e. ☐ Yes ☐ No ☐ N/A |

| | | |
|---|---|---|
| SI-5 | Does your organization?<br>a. Receive information security alerts, advisories, and directives on an ongoing basis?<br>b. Generate internal security alerts, advisories, and directives as deemed necessary?<br>c. Disseminate security alerts, advisories, and directives to defined personnel or roles?<br>d. Implement security directives in accordance with established time frames? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A<br>c. ☐ Yes ☐ No ☐ N/A<br>d. ☐ Yes ☐ No ☐ N/A |
| SI-7 | Does your organization employ integrity verification tools to detect unauthorized changes to software, firmware, and information? | ☐ Yes ☐ No ☐ N/A |
| SI-8<br>SI-8(1)<br>SI-8(2) | Does your organization:<br>a. Employ spam protection mechanisms at information system entry and exit points to detect and act on unsolicited messages?<br>b. Update spam protection mechanisms when new releases are available?<br>c. Centrally manage spam protection mechanisms?<br>d. Automatically update spam protection mechanisms? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A<br>c. ☐ Yes ☐ No ☐ N/A<br>d. ☐ Yes ☐ No ☐ N/A |
| SI-10 | Does your organization check the validity of defined information inputs for accuracy, completeness, validity, and authenticity as close to the point of origin as possible? | ☐ Yes ☐ No ☐ N/A |
| SI-11 | Does your organization information system:<br>a. Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries?<br>b. Reveal error messages only to defined personnel or roles? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A |

**If "No" or "N/A" was selected for any of the above listed control-specific questions, please provide a brief rationale explaining why your organization has chosen not to implement the applicable control. Please add rows as needed.**

| *Control(s) Referenced* | *Rationale* | *Confirm Box Selected* |
|---|---|---|
| SI-? | Click or tap here to enter text. | ☐ No ☐ N/A |
| SI-? | Click or tap here to enter text. | ☐ No ☐ N/A |

**As support for the answers above, please upload specific organizational policy and/or procedural document(s) to the secure QECP Salesforce Portal. In addition, please specify the control(s) referenced, document title, page/section reference, and last reviewed date to support future requests for evidence if required. Please add rows as needed.**

| *Control(s) Referenced* | *Document Title, Page/Section Reference* | *Last Reviewed Date* |
|---|---|---|
| SI-? | Click or tap here to enter text. | |
| SI-? | Click or tap here to enter text. | |

## 18. Program Management (PM)

| | | |
|---|---|---|
| PM-1 | Does your organization:<br>a. Develop and disseminate an organization-wide information security program that is approved by a senior official with responsibility and accountability for organizational risk?<br>b. Is that program reviewed and updated (as necessary) at least every 365 days? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A |
| PM-2 | Does your organization have a Chief Information Security Officer appointed to manage the security program, or similarly recognized official? | ☐ Yes ☐ No ☐ N/A |
| PM-4 | Does your organization have a process that tracks, documents, and rectifies findings? | ☐ Yes ☐ No ☐ N/A |
| PM-12 | Does your organization implement an insider threat program that includes a cross-discipline insider threat incident handling team? | ☐ Yes ☐ No ☐ N/A |

**If "No" or "N/A" was selected for any of the above listed control-specific questions, please provide a brief rationale explaining why your organization has chosen not to implement the applicable control. Please add rows as needed.**

| *Control(s) Referenced* | *Rationale* | *Confirm Box Selected* |
|---|---|---|
| PM-? | Click or tap here to enter text. | ☐ No ☐ N/A |
| PM-? | Click or tap here to enter text. | ☐ No ☐ N/A |

## 19. Authority and Purpose (AP)

| | | |
|---|---|---|
| AP-CMS-1 | Does your organization determine and document the legal authority that permits the collection, use, maintenance, and sharing of PII, either generally or in support of specific programs and the needs of information systems? | ☐ Yes ☐ No ☐ N/A |

**If "No" or "N/A" was selected for the above listed control-specific question, please provide a brief rationale explaining why your organization has chosen not to implement the applicable control.**

| *Control(s) Referenced* | *Rationale* | *Confirm Box Selected* |
|---|---|---|
| AP-CMS-1 | Click or tap here to enter text. | ☐ No ☐ N/A |

## 20. Accountability, Audit and Risk Management (AR)

| | | |
|---|---|---|
| AR-1 | Does your organization:<br>a. Appoint a Senior Official for Privacy (SOP) accountable for developing, implementing, and maintaining an organization-wide governance and privacy program to ensure compliance with all applicable laws and regulations regarding the collection, use, maintenance, sharing, and disposal of PII by programs and information systems? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A<br>c. ☐ Yes ☐ No ☐ N/A<br>d. ☐ Yes ☐ No ☐ N/A<br>e. ☐ Yes ☐ No ☐ N/A |

| | | |
|---|---|---|
| | b. Monitor federal privacy laws and policy for changes that affect the privacy program?<br>c. Allocate an appropriate budget and staffing resources to implement and operate the organization-wide privacy program?<br>d. Develop a strategic organizational privacy plan for implementing applicable privacy controls, policies, and procedures?<br>e. Develop, disseminate, and implement operational privacy policies and procedures that govern the appropriate privacy and security controls for programs, information systems, or technologies involving PII?<br>f. Update privacy plan, policies, and procedures, as required to address changing requirements, but no less often than every 2 years? | f. ☐ Yes ☐ No ☐ N/A |
| AR-3 | Does your organization:<br>a. Establish privacy roles, responsibilities, and access requirements for contractors and service providers?<br>b. Include privacy requirements in contracts and other acquisition-related documents?<br>c. Review every 2 years, a random sample of contracts to ensure that the contracts include clauses that make all requirements and penalty provisions of the Privacy Act apply to the contractor or service provider and its personnel? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A<br>c. ☐ Yes ☐ No ☐ N/A |
| AR-4 | Does your organization:<br>a. Monitor and audit privacy controls at least every 365 days to ensure effective implementation?<br>b. Monitor for changes to applicable privacy laws, regulations, and policy affecting internal privacy policy no less often than once every 365 days to ensure internal privacy policy remains effective?<br>c. Document, track, and ensure mitigation of corrective actions identified through monitoring or auditing? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A<br>c. ☐ Yes ☐ No ☐ N/A |
| AR-5 | Does your organization:<br>a. Develop, implement, and routinely update a comprehensive privacy training and awareness strategy?<br>b. Administer basic and targeted privacy training no less often than once every 365 days?<br>c. Ensure that personnel certify (manually or electronically) acceptance of responsibilities for privacy requirements no less often than once every 365 days? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A<br>c. ☐ Yes ☐ No ☐ N/A |
| AR-8 | Does your organization ensure that an accurate accounting of information disclosures is kept for the life of the record or 5 years after the disclosure was made, whichever is longer? | ☐ Yes ☐ No ☐ N/A |
| AR-CMS-1 | Does your organization:<br>a. Have an Accountability, Audit, and Risk Management policy (and subsequent procedures to facilitate the implementation of that policy) that identifies the purpose, scope, roles, | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A |

| | | |
|---|---|---|
| | responsibilities, and management commitment for all parties using CMS data?<br>b. Is that policy and subsequent procedures reviewed and updated (as necessary) at least every 2 years? | |

**If "No" or "N/A" was selected for any of the above listed control-specific questions, please provide a brief rationale explaining why your organization has chosen not to implement the applicable control. Please add rows as needed.**

| *Control(s) Referenced* | *Rationale* | *Confirm Box Selected* |
|---|---|---|
| AR-? | Click or tap here to enter text. | ☐ No ☐ N/A |
| AR-? | Click or tap here to enter text. | ☐ No ☐ N/A |

## 21. Data Quality and Integrity (DI)

| | | |
|---|---|---|
| DI-CMS-1 | Does your organization:<br>a. Have a Data Quality and Integrity policy (and subsequent procedures to facilitate the implementation of that policy) that addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance for all parties using CMS data?<br>b. Is that policy and subsequent procedures reviewed and updated (as necessary) at least every 2 years? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A |

**If "No" or "N/A" was selected for any of the above listed control-specific questions, please provide a brief rationale explaining why your organization has chosen not to implement the applicable control. Please add rows as needed.**

| *Control(s) Referenced* | *Rationale* | *Confirm Box Selected* |
|---|---|---|
| DI-CMS-1 | Click or tap here to enter text. | ☐ No ☐ N/A |

## 22. Data Minimization and Retention (DM)

| | | |
|---|---|---|
| DM-1(1) | Does your organization, where feasible and within the limits of technology and the law, locate and remove/redact specified PII and/or uses anonymization and de-identification techniques to permit authorized use of the retained information while reducing its sensitivity and reducing the risk resulting from disclosure? | ☐ Yes ☐ No ☐ N/A |
| DM-2 | Does your organization:<br>a. Retain each collection of PII for the time period specified by the NARA-approved Records Schedule?<br>b. Dispose of, destroy, erase, and/or anonymize the PII in a manner that prevents loss, theft, misuse, or unauthorized access?<br>c. Use FIPS-validated techniques or methods to ensure secure deletion or destruction of PII (including originals, copies, and archived records)? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A<br>c. ☐ Yes ☐ No ☐ N/A |

| | | |
|---|---|---|
| DM-3<br>DM-3(1) | Does your organization:<br>a. Develop policies and procedures that minimize the use of PII for testing, training, and research?<br>b. Implement controls to protect PII used for testing, training, and research?<br>c. Where feasible, use techniques to minimize the risk to privacy of using PII for research, testing, or training? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A<br>c. ☐ Yes ☐ No ☐ N/A |
| DM-CMS-1 | Does your organization:<br>a. Have a Data Minimization and Retention policy (and subsequent procedures to facilitate the implementation of that policy) that addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance for all parties using CMS data?<br>b. Is that policy and subsequent procedures reviewed and updated (as necessary) at least every 2 years? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A |

**If "No" or "N/A" was selected for any of the above listed control-specific questions, please provide a brief rationale explaining why your organization has chosen not to implement the applicable control. Please add rows as needed.**

| *Control(s) Referenced* | *Rationale* | *Confirm Box Selected* |
|---|---|---|
| DM-? | Click or tap here to enter text. | ☐ No ☐ N/A |
| DM-? | Click or tap here to enter text. | ☐ No ☐ N/A |

## 23. Individual Participation and Redress (IP)

| | | |
|---|---|---|
| IP-CMS-1 | Does your organization:<br>a. Have an Individual Participation and Redress policy (and subsequent procedures to facilitate the implementation of that policy) that addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance for all parties using CMS data?<br>b. Is that policy and subsequent procedures reviewed and updated (as necessary) at least every 2 years? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A |

**If "No" or "N/A" was selected for any of the above listed control-specific questions, please provide a brief rationale explaining why your organization has chosen not to implement the applicable control. Please add rows as needed.**

| *Control(s) Referenced* | *Rationale* | *Confirm Box Selected* |
|---|---|---|
| IP-CMS-1 | Click or tap here to enter text. | ☐ No ☐ N/A |

## 24. Security (SE)

| | | |
|---|---|---|
| SE-1 | Does your organization: | a. ☐ Yes ☐ No ☐ N/A |

| | | |
|---|---|---|
| | a. Establish, maintain, and update every 365 days, an inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing PII?<br>b. Provide each update of the PII inventory to the appropriate personnel? | b. ☐ Yes ☐ No ☐ N/A |
| SE-2 | Does your organization:<br>a. Develop and implement a Privacy Incident and Breach Response Plan?<br>b. Provide an organized and effective response to privacy incidents and breaches? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A |
| SE-CMS-1 | Does your organization:<br>a. Have a Security policy (and subsequent procedures to facilitate the implementation of that policy) that addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance for all parties using CMS data?<br>b. Is that policy and subsequent procedures reviewed and updated (as necessary) at least every 2 years? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A |

**If "No" or "N/A" was selected for any of the above listed control-specific questions, please provide a brief rationale explaining why your organization has chosen not to implement the applicable control. Please add rows as needed.**

| *Control(s) Referenced* | *Rationale* | *Confirm Box Selected* |
|---|---|---|
| SE-? | Click or tap here to enter text. | ☐ No ☐ N/A |
| SE-? | Click or tap here to enter text. | ☐ No ☐ N/A |

## 25. Transparency (TR)

| | | |
|---|---|---|
| TR-3 | Does your organization:<br>a. Ensure that the public has access to information about its privacy activities and can communicate with its Senior Official for Privacy (SOP)?<br>b. Ensure that its privacy practices are publicly available through organizational websites or otherwise? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A |
| TR-CMS-1 | Does your organization:<br>a. Have a Transparency policy (and subsequent procedures to facilitate the implementation of that policy) that addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance for all parties using CMS data?<br>b. Is that policy and subsequent procedures reviewed and updated (as necessary) at least every 2 years? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A |

| **If "No" or "N/A" was selected for any of the above listed control-specific questions, please provide a brief rationale explaining why your organization has chosen not to implement the applicable control. Please add rows as needed.** | | |
|---|---|---|
| *Control(s) Referenced* | *Rationale* | *Confirm Box Selected* |
| TR-? | Click or tap here to enter text. | ☐ No ☐ N/A |
| TR-? | Click or tap here to enter text. | ☐ No ☐ N/A |

### 26. Use Limitation (UL)

| | | |
|---|---|---|
| UL-1<br>UL-2 | Does your organization use PII or PHI:<br>a. Internally – only for authorized purpose(s) identified in the Privacy Act?<br>b. Externally – only for authorized purposes by permission of an authorized Business Associate Agreement (BAA) with third-parties, specifically describing the PII covered and purposes for which it may be used? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A |
| UL-CMS-1 | Does your organization:<br>a. Have a Use Limitation policy (and subsequent procedures to facilitate the implementation of that policy) that addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance for all parties using CMS data?<br>b. Is that policy and subsequent procedures reviewed and updated (as necessary) at least every 2 years? | a. ☐ Yes ☐ No ☐ N/A<br>b. ☐ Yes ☐ No ☐ N/A |

| **If "No" or "N/A" was selected for any of the above listed control-specific questions, please provide a brief rationale explaining why your organization has chosen not to implement the applicable control. Please add rows as needed.** | | |
|---|---|---|
| *Control(s) Referenced* | *Rationale* | *Confirm Box Selected* |
| UL-? | Click or tap here to enter text. | ☐ No ☐ N/A |
| UL-? | Click or tap here to enter text. | ☐ No ☐ N/A |

## F. Overall Attestations and Audit Agreement

By the Security or Privacy Officer's attestations and signature below, the applicant validates that the responses and the information provided on this form and any other supporting documents related to this review are in fact true, complete, and accurate. All related policies, procedures, and controls specified above may be subject to **audit** by CMS or CMS appointed personnel, including possible on-site engagements. If required, this audit will be at the cost of the applicant.

| | |
|---|---|
| Our organization is utilizing a Cloud Service Provider (CSP), and understand that security and compliance are a shared responsibility between us, the customer, and the CSP. As the customer, we have responsibility for security 'in' the cloud (customer data, applications, | ☐ Yes ☐ No ☐ N/A |

| | |
|---|---|
| identity & access management, etc.), while the CSP has responsibility for security 'of' the cloud (compute, storage, networking, regions, availability zones, etc.). | |

| | |
|---|---|
| I have reviewed all information, either presented above or attached to this review, and attest that is in fact true, complete, and accurate. | ☐ Yes ☐ No |

| | |
|---|---|
| Name of QE | <Insert QE Name> |
| Name of Person Attesting | <Insert Name of Person Attesting> |
| Title of Person Attesting | <Insert Title of Person Attesting (Privacy or Security Officer of QE)> |
| Signature of Person Attesting | <Insert Digital Signature of Person Attesting> |
| Date | <Insert Attestation Date> |