Qualified Entity Certification Program

Data Security Review

Final, Version 2.0

Table of Contents

List of Tables

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.

Under the QECP, CMS certifies Qualified Entities (QEs) to receive these data and monitors certified QEs. As part of the Data Security Review (DSR), or Phase 2 of the overall certification process, the organization must complete the following attestation questionnaire.

The QECP DSR follows a tailored framework modeled after the CMS Acceptable Risk Safeguards (ARS) Version 5.1, 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 on the QECP website.
- If you are utilizing any vendors (e.g., Cloud Service Provider (CSP), colocation facility, data management vendor), show proof of an executed Business Associate Agreement (BAA) between your organization and those vendors. This documentation should show the names of the parties involved, effective dates of the agreement, and appropriate signatures. Please do not attach generic documents.
- 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 organization and data details, key contacts, and relevant data breach incidents in Sections A, B, and C.
2. Complete Section D by attesting to each security/privacy control question (i.e., selecting Yes or No). Please provide a narrative statement justification in the rationale section for each No or NA answer.
3. Complete Section E 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 & Data Details

Directions: The 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 overall remains responsible for ensuring that controls are in place and operating effectively for all parties, including data custodians and/or partners.

Please identify the organization(s) participating in the QECP application. Note which physical location will store the identifiable data and which organizations will access identifiable data. 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.

If a CSP will be used by either the QE or Data Custodian to store or process CMS data, please note that in Table 1.

Table 1: Organization Information

Item	Response Data
QE Organization Name	QE Organization Name
QE Address	QE Address
Does the QE store identifiable data?	Yes or No
Does the QE access identifiable data?	Yes or No
Computing Environment Type	CSP On-site (Facility owned by QE) Off-site (Colocation or Leased Space) Hybrid: Uses CSP & On-site/Off-site
Computing Environment Address(es)	Computing Environment Address(es)
Data Custodian Organization Name	Data Custodian Name or Not Applicable (NA) if the QE Organization is the Data Custodian
Does the Data Custodian store identifiable data?	Yes or No
Does the Data Custodian access identifiable data?	Yes or No
Data Custodian Address	Data Custodian Address

B. Key Individuals

Directions: Please identify key individuals for the QE organization.

Table 2: Key Individuals

Item	Response Data	Description
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 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.

Optional: NA. Our organization has not experienced any data security breaches during the last 10 years.

Table 3: Data Security Breaches

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

D. Security and Privacy Controls

Directions: For each question, please attest to whether your organization has implemented the listed control, focusing on the system(s) that will contain CMS data. If No is selected, please provide rationale at the end of each subsection.

Table 4: Access Control (AC)

Control (s)	Item	Response Data
AC-1	Does your organization have an Access Control policy (and subsequent procedures to facilitate the implementation of that policy) that addresses the purpose, scope, responsibility, management commitment, coordination among organizational entities, and compliance for all parties using CMS data? Is the policy disseminated to the appropriate personnel or roles? Is that policy reviewed and updated (as necessary) annually?	Yes or No
AC-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?	Yes or No
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 or No
AC-4	Does your organization ensure it controls information flow within the system and any interconnected (internal or external) systems?	Yes or No
AC-5	Does your organization ensure the information system separates the duties of users?	Yes or No
AC-6 AC-6(1) AC-6(7) AC-6(9)	Does your organization ensure that only authorized users have permissions required to perform their job duties by disabling non-essential functions; ensure security functions are explicitly authorized; review privileges assigned to users every 90 days; ensure that authorized users use their own account to access the system; escalate privileges to perform administrative functions; and log all privileged account usage activities?	Yes or No
AC-7	Does your organization ensure that the information system enforces the automatic disabling/locking of accounts for 1 hour after five invalid login attempts during a 120-minute time window?	Yes or No
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 or No
AC-11	Does your organization ensure that user sessions lock after 15 minutes of inactivity and/or are automatically disconnected under specified circumstances; and ensure that the information system conceals, via the session lock, information previously visible on the display with a publicly viewable image?	Yes or No
AC-12	Does your organization ensure that the information system automatically terminates a user session after defined conditions or trigger events are met?	Yes or No
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 or No

Control (s)	Item	Response Data
AC-17 AC-17(1) AC-17(2) AC-17(3) AC-17(4)	Does your organization's remote connections have usage restrictions; connection requirements such as cryptography and 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?	Yes or No
AC-18	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 or No
AC-19	Does your organization establish configuration requirements, connection requirements, and implementation guidance for mobile devices?	Yes or No
AC-20 AC-20(1) AC-20(2)	Does your organization ensure that the information system does not allow external systems to process, store, or transmit system information unless explicitly authorized?	Yes or No
AC-21	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?)	Yes or No

If No 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.

Table 5: AC Rationale

Control (s) Referenced	Rationale
AC-	Rationale

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.

Table 6: AC Rationale Document(s)

Control (s) Referenced	Document, Title, Page/Section Reference
AC-	Document, Title, Page/Section Reference

Table 7: Awareness and Training (AT)

Control (s)	Item	Response Data
AT-1	Does your organization have an Awareness and Training policy (and subsequent procedures to facilitate the implementation of that policy) that addresses the purpose, scope, responsibility, management commitment, coordination among organizational entities, and compliance for all parties using CMS data? Is the policy disseminated to the appropriate personnel or roles? Is that policy reviewed and updated (as necessary) annually?	Yes or No
AT-2	Does your organization ensure that system users (including managers, senior executives, and contractors) receive security and privacy literacy training as part of initial training for 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 that training?	Yes or No
AT-2(2) AT-2(3)	Does your organization ensure that the security training program includes modules for security and privacy awareness, insider threat identification, and social engineering?	Yes or No
AT-3	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?	Yes or No
AT-3(5)	Does your organization provide personnel (both contractor and employee) with initial and annual training in the employment and operation of personally identifiable information processing and transparency controls.	Yes or No
AT-4	Does your organization retain individual security training records for a minimum of 5 years after the individual completes each training?	Yes or No

If No 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.

Table 8: AT Rationale

Control (s) Referenced	Rationale
AT-	Rationale

Table 9: Audit and Accountability (AU)

Control (s)	Item	Response Data
AU-1	Does your organization have an Auditing and Accountability policy (and subsequent procedures to facilitate the implementation of that policy) that addresses the purpose, scope, responsibility, management commitment, coordination among organizational entities, and compliance for all parties using CMS data? Is the policy disseminated to the appropriate personnel or roles? Is that policy reviewed and updated (as necessary) annually?	Yes or No

Control (s)	Item	Response Data
AU-2	Does your organization's information system have the capability to log events in support of the audit function including: User log on and log off (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 log on from different workstations; override of access control mechanisms; startup/shutdown of audit logging services; and audit logging service configuration changes?	Yes or No
AU-3 AU-3(1)	Does your organization ensure that the audit records from the information system contain the following metadata to support the detection, monitoring, investigation, response, and remediation of security and privacy incidents: Date and time of the event (e.g., timestamp); process identifier or system component (e.g., software, hardware) generating the event; user or account that initiated the event (unique username/identifier); event type; event outcome (success/failure); any privileged system functions executed; process creation information (command line captures if applicable)?	Yes or No
AU-6(3)	Does your organization analyze and correlate audit records across different repositories to gain organization-wide situational awareness?	Yes or No
AU-7(1)	Does your organization ensure audit records are searchable?	Yes or No
AU-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 Network Time Protocol (NTP) server, National Institute of Standards and Technology (NIST) time service, etc.) and that audit records use the internal system clocks to generate a time stamp?	Yes or No
AU-9 AU-9(4)	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?	Yes or No
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 or No

If No 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.

Table 10: AU Rationale

Control (s) Referenced	Rationale
AU-	Rationale

Table 11: Security Assessment and Authorization (CA)

Control (s)	Item	Response Data
CA-1	Does your organization have a Security Assessment and Authorization policy (and subsequent procedures to facilitate the implementation of that policy) that addresses the purpose, scope, responsibility, management commitment, coordination among organizational entities, and compliance for all parties using CMS data? Is the policy disseminated to the appropriate personnel or roles? Is that policy reviewed and updated (as necessary) annually?	Yes or No
CA-2	Does your organization develop an information security and privacy control assessment plan that describes the scope of the assessment and contains the controls under assessment, assessment procedures to determine control effectiveness, the assessment environment/team/roles and responsibilities?	Yes or No
CA-2(1)	Does your organization conduct information security and privacy control assessments annually using independent assessors?	Yes or No
CA-3 CA-9	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?	Yes or No
CA-7	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?	Yes or No

If No 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.

Table 12: CA Rationale

Control (s) Referenced	Rationale
CA-	Rationale

Table 13: Configuration Management (CM)

Control (s)	Item	Response Data
CM-1	Does your organization have a Configuration Management policy (and subsequent procedures to facilitate the implementation of that policy) that addresses the purpose, scope, responsibility, management commitment, coordination among organizational entities, and compliance for all parties using CMS data? Is the policy disseminated to the appropriate personnel or roles? Is that policy reviewed and updated (as necessary) annually?	Yes or No
CM-2	Does your organization ensure that the information system has a current baseline configuration image for hosts within the system?	Yes or No
CM-3	Does your organization track, review, approve or disapprove, and log changes to organizational information systems?	Yes or No

Control (s)	Item	Response Data
CM-5	Does your organization ensure that the information system uses physical and logical access restrictions to prevent unauthorized changes?	Yes or No
CM-6	Does your organization establish and document configuration settings for components employed within the system using the latest security baseline configurations?	Yes or No
CM-7 CM-7(5)	Does your organization ensure that the configuration of the information system allows only essential functions, software, ports, protocols, and applications (whitelisting)?	Yes or No
CM-8 CM-8(1)	Does your organization maintain and review at least every 180 days an up-to-date system inventory to include all boundary components, such as: Each component's unique identifier and/or serial number; the information system of which the component is a part; the type of information system component (e.g., server, desktop, application); the manufacturer/model information; the operating system type and version/service pack level; the presence of virtual machines; the application software version/license information; the physical location (e.g., building/room number); the logical location (e.g., Internet Protocol (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?	Yes or No
CM-11	Does your organization ensure that the information system prevents users from installing software through user policies?	Yes or No

If No 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.

Table 14: CM Rationale

Control (s) Referenced	Rationale
CM-	Rationale

Table 15: Contingency Planning (CP)

Control (s)	Item	Response Data
CP-1	Does your organization have a Contingency Planning policy (and subsequent procedures to facilitate the implementation of that policy) that addresses the purpose, scope, responsibility, management commitment, coordination among organizational entities, and compliance for all parties using CMS data? Is the policy disseminated to the appropriate personnel or roles? Is that policy reviewed and updated (as necessary) annually?	Yes or No
CP-9	Does your organization perform weekly and/or daily backups of user-level information, system-level information, and information system documentation? Does your organization protect the confidentiality, integrity, and availability of backups containing CMS data?	Yes or No

If No 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.

Table 16: CP Rationale

Control (s) Referenced	Rationale
CP-	Rationale

Table 17: Identification and Authentication (IA)

Control (s)	Item	Response Data
IA-1	Does your organization have an Identification and Authentication policy (and subsequent procedures to facilitate the implementation of that policy) that addresses the purpose, scope, responsibility, management commitment, coordination among organizational entities, and compliance for all parties using CMS data? Is the policy disseminated to the appropriate personnel or roles? Is that policy reviewed and updated (as necessary) annually?	Yes or No
IA-2 IA-2(1) IA-2(2) IA-12	Does your organization ensure that the information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users), and implements multifactor authentication (MFA) for network access to privileged and non-privileged accounts?	Yes or No
IA-3 IA-5 IA-5(1)	Does your organization uniquely identify and authenticate devices prior to granting access to organizational systems through effective identity proofing and authentication processes? Does your organization establish requirements for device authenticators; define reuse conditions; and set minimum and maximum lifetimes for each authenticator type to be used?	Yes or No
IA-4	Does your organization successfully assign unique identifiers to users and devices; prevent reuse of identifiers for 3 years; and disable identifiers after 60 days of inactivity?	Yes or No
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 or No

If No 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.

Table 18: IA Rationale

Control (s) Referenced	Rationale
IA-	Rationale

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.

Table 19: IA Rationale Document(s)

Control (s) Referenced	Document, Title, Page/Section Reference
IA-	Document, Title, Page/Section Reference

Table 20: Incident Response (IR)

Control (s)	Item	Response Data
IR-1	Does your organization have an Incident Response policy (and subsequent procedures to facilitate the implementation of that policy) that addresses the purpose, scope, responsibility, management commitment, coordination among organizational entities, and compliance for all parties using CMS data? Is the policy disseminated to the appropriate personnel or roles? Is that policy reviewed and updated (as necessary) annually?	Yes or No
IR-2	Does your organization ensure that employees who have incident response duties complete incident response training within 1 month of assuming the role and annually thereafter, and that incident response training content is reviewed and updated annually?	Yes or No
IR-3	Does your organization test the incident response capability of the information system annually to determine the organization's incident response effectiveness, and document its findings?	Yes or No
IR-4	Does your organization implement an incident handling capability, coordinate incident handling activities with contingency planning activities, and incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises?	Yes or No
IR-5	Does your organization track and document all physical, information security, and privacy incidents?	Yes or No
IR-6	Does your organization require personnel to report actual or suspected security and privacy incidents?	Yes or No
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 or No

Control (s)	Item	Response Data
IR-8	Does your organization have an incident response plan that: Provides the organization with a roadmap for implementing its incident response (IR) 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 annually 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?	Yes or No
IR-8(1)	Does your organization include the following 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.	Yes or No

If No 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.

Table 21: IR Rationale

Control (s) Referenced	Rationale
IR-	Rationale

Table 22: Maintenance (MA)

Control (s)	Item	Response Data
MA-1	Does your organization have a Maintenance policy (and subsequent procedures to facilitate the implementation of that policy) that addresses the purpose, scope, responsibility, management commitment, coordination among organizational entities, and compliance for all parties using CMS data? Is the policy disseminated to the appropriate personnel or roles? Is that policy reviewed and updated (as necessary) annually?	Yes or No

Control (s)	Item	Response Data
MA-3 MA-3(1) MA-3(2)	Does your organization approve, control, and monitor information system maintenance tools; inspect the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications; and check media containing diagnostic and test programs for malicious code before the media are used in the information system?	Yes or No

If No 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.

Table 23: MA Rationale

Control (s) Referenced	Rationale
MA-	Rationale

Table 24: Media Protection (MP)

Control (s)	Item	Response Data
MP-1	Does your organization have a Media Protection policy (and subsequent procedures to facilitate the implementation of that policy) that addresses the purpose, scope, responsibility, management commitment, coordination among organizational entities, and compliance for all parties using CMS data? Is the policy disseminated to the appropriate personnel or roles? Is that policy reviewed and updated (as necessary) annually?	Yes or No
MP-3	Does your organization mark information system media based on the sensitivity of information the media holds?	Yes or No
MP-4	Does your organization physically control and securely store digital and non-digital media within controlled areas; and protect information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures?	Yes or No
MP-5	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?	Yes or No
MP-6 MP-6(1)	Does your organization 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; and review, approve, track, document, and verify media sanitization and disposal actions?	Yes or No
MP-7	Does your organization prohibit the use of personally owned storage media and ensure that allowed portable storage devices have an identified owner (e.g., designated personnel or organization)?	Yes or No

If No 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.

Table 25: MP Rationale

Control (s) Referenced	Rationale
MP-	Rationale

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.

Table 26: MP Rationale Document(s)

Control (s) Referenced	Document, Title, Page/Section Reference
MP-	Document, Title, Page/Section Reference

Table 27: Physical and Environmental Protection (PE)

Control (s)	Item	Response Data
PE-1	Does your organization have a Physical and Environmental Protection policy (and subsequent procedures to facilitate the implementation of that policy) that addresses the purpose, scope, responsibility, management commitment, coordination among organizational entities, and compliance for all parties using CMS data? Is the policy disseminated to the appropriate personnel or roles? Is that policy reviewed and updated (as necessary) annually?	Yes or No
PE-2	Does your organization do the following: Develop, approve, and maintain a list of individuals with authorized access to the facility where the system resides; issue authorization credentials for facility access; review the access list detailing authorized facility access by individuals within every, 180 days; and remove individuals from the facility access list when access is no longer required?	Yes or No

Control (s)	Item	Response Data
PE-3	Does your organization ensure it: Verifies individual access authorizations before granting access to the facility; controls ingress/egress to the facility using guards and/or defined physical access control systems/devices (defined in the applicable security plan); maintains physical access audit logs for defined entry/exit points (defined in the applicable security plan); provides defined security safeguards (defined in the applicable security plan) to control access to areas within the facility officially designated as publicly accessible; escorts visitors and monitors visitor activity in defined circumstances requiring visitor escorts and monitoring (defined in the applicable security plan); secures keys, combinations, and other physical access devices; inventories defined physical access devices (defined in the applicable security plan), no less often than every 90 days; and changes combinations and keys for defined high-risk entry/exit points (defined in the applicable security plan) annually, and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated?	Yes or No
PE-4	Does your organization ensure that telephone and network hardware and transmission lines (e.g., wiring closets, patch panels, etc.) are protected?	Yes or No
PE-6	Does your organization monitor physical access to the facility where CMS data resides and respond to physical security incidents; review physical access logs weekly and upon occurrence of security incidents; and coordinate results of reviews and investigations with the organization's incident response capability?	Yes or No
PE-8	Does your organization maintain visitor access records to the facility for 2 years; and review visitor access records no less often than monthly?	Yes or No

If No 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.

Table 28: PE Rationale

Control (s) Referenced	Rationale
PE-	Rationale

Table 29: Planning (PL)

Control (s)	Item	Response Data
PL-1	Does your organization have a Planning policy (and subsequent procedures to facilitate the implementation of that policy) that addresses the purpose, scope, responsibility, management commitment, coordination among organizational entities, and compliance for all parties using CMS data? Is the policy disseminated to the appropriate personnel or roles? Is that policy reviewed and updated (as necessary) annually?	Yes or No

Control (s)	Item	Response Data
PL-2	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?	Yes or No
PL-4	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?	Yes or No

If No 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.

Table 30: PL Rationale

Control (s) Referenced	Rationale
PL-	Rationale

Table 31: Personnel Security

Control (s)	Item	Response Data
PS-1	Does your organization have a Personnel Security policy (and subsequent procedures to facilitate the implementation of that policy) that addresses the purpose, scope, responsibility, management commitment, coordination among organizational entities, and compliance for all parties using CMS data? Is the policy disseminated to the appropriate personnel or roles? Is that policy reviewed and updated (as necessary) annually?	Yes or No
PS-3	Does your organization follow organizational policy regarding background checks and screening for employees with access to CMS data?	Yes or No
PS-4	Does your organization upon termination of an individual's 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 1 calendar day; and immediately escort employees terminated for cause out of the organization?	Yes or No
PS-6	Does your organization develop and document access agreements (e.g., nondisclosure, acceptable use, rules of behavior, and conflict-of-interest agreements) for organizational systems; review and update the access agreements annually; and verify that individuals requiring access to organizational information and systems sign appropriate access agreements (paper or electronic) prior to being granted access?	Yes or No

Control (s)	Item	Response Data
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 or No
PS-8	Does your organization ensure that the organization has a formal sanction process for employees who violate security policies or procedures?	Yes or No

If No 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.

Table 32: PS Rationale

Control (s) Referenced	Rationale
PS-	Rationale

Table 33: Risk Assessment (RA)

Control (s)	Item	Response Data
RA-1	Does your organization have a Risk Assessment policy (and subsequent procedures to facilitate the implementation of that policy) that addresses the purpose, scope, responsibility, management commitment, coordination among organizational entities, and compliance for all parties using CMS data? Is the policy disseminated to the appropriate personnel or roles? Is that policy reviewed and updated (as necessary) annually?	Yes or No
RA-3	Does your organization do the following: 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; document risk assessment results in the applicable security plan; review risk assessment results annually; disseminate risk assessment results to affected stakeholders and Business Owners; update the risk assessment at a minimum every 3 years, or whenever there are significant changes to the system?	Yes or No
RA-5	Does your organization use an automated vulnerability scanner to scan for vulnerabilities in the information system and hosted systems no less often than once every 72 hours and when new vulnerabilities are identified?	Yes or No

If No 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
RA-	Rationale

Table 34: System and Services Acquisition (SA)

Control (s)	Item	Response Data
SA-1	Does your organization have a System and Services Acquisition policy (and subsequent procedures to facilitate the implementation of that policy) that addresses the purpose, scope, responsibility, management commitment, coordination among organizational entities, and compliance for all parties using CMS data? Is the policy disseminated to the appropriate personnel or roles? Is that policy reviewed and updated (as necessary) annually?	Yes or No
SA-5	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?	Yes or No
SA-8	Does your organization apply security and privacy engineering principles (consistent with NIST Special Publication (SP) 800-160 Volume 1) in specification, design, development, implementation, and modification of the system and system components?	Yes or No
SA-9	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 or No

If No 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.

Table 35: SA Rationale

Control (s) Referenced	Rationale
SA-	Rationale

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.

Table 36: SA Rationale Document(s)

Control (s) Referenced	Document, Title, Page/Section Reference
SA-	Document, Title, Page/Section Reference

Table 37: System and Communications Protection (SC)

Control (s)	Item	Response Data
SC-1	Does your organization have a System and Communications Protection policy (and subsequent procedures to facilitate the implementation of that policy) that addresses the purpose, scope, responsibility, management commitment, coordination among organizational entities, and compliance for all parties using CMS data? Is the policy disseminated to the appropriate personnel or roles? Is that policy reviewed and updated (as necessary) annually?	Yes or No
SC-2	Does your organization ensure that administrative and regular user interfaces are separate?	Yes or No
SC-7	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 (e.g., firewall, Intrusion Detection System (IDS)/Intrusion Prevention System (IPS))?	Yes or No
SC-7(5)	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 (i.e., deny all, permit by exception)?	Yes or No
SC-7(7)	Does your organization prevent split tunneling for remote devices connecting to organizational systems unless the split tunnel is securely provisioned using defined security safeguards (i.e., the use of Virtual Private Network (VPN) for remote connections, sufficiently provisioned with appropriate security and privacy controls)?	Yes or No
SC-8 SC-13 SC-28	Does your organization ensure that the information systems use Federal Information Processing Standards (FIPS) 140-2 validated cryptographic modules for transmission of data-in-motion and/or data-at-rest?	Yes or No
SC-10	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?	Yes or No
SC-12	Does your organization have a centralized cryptographic key management system that complies with organizational standards?	Yes or No
SC-15	Does your organization prohibit running collaborative computing mechanisms (e.g., networked white boards, cameras, and microphones) unless explicitly authorized?	Yes or No

If No 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.

Table 38: SC Rationale

Control (s) Referenced	Rationale
SC-	Rationale

Table 39: System and Information Integrity (SI)

Control (s)	Item	Response Data
SI-1	Does your organization have a System and Information Integrity policy (and subsequent procedures to facilitate the implementation of that policy) that addresses the purpose, scope, responsibility, management commitment, coordination among organizational entities, and compliance for all parties using CMS data? Is the policy disseminated to the appropriate personnel or roles? Is that policy reviewed and updated (as necessary) annually?	Yes or No
SI-2	Does your organization: Identify, report, and correct 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?	Yes or No
SI-3	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? Does your organization's information system use malicious code protection that has up-to-date virus definitions and scans important file systems every 12 hours and full system every 72 hours?	Yes or No
SI-4 SI-4(4)	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?	Yes or No
SI-5	Does your organization receive information security alerts, advisories, and directives on an ongoing basis; generate internal security alerts, advisories, and directives as deemed necessary; disseminate security alerts, advisories, and directives to defined personnel or roles; and implement security directives in accordance with established time frames?	Yes or No
SI-7	Does your organization employ integrity verification tools to detect unauthorized changes to software, firmware, and information?	Yes or No
SI-8	Does your organization employ spam filters for email servers hosted within the system boundary, if applicable?	Yes or No
SI-10	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?	Yes or No
SI-11	Does your organization's information system generate error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries; and reveal error messages only to defined personnel or roles?	Yes or No

If No 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.

Table 40: SI Rationale

Control (s) Referenced	Rationale
SI-	Rationale

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.

Table 41: SI Rationale Document(s)

Control (s) Referenced	Document, Title, Page/Section Reference
SI-	Document, Title, Page/Section Reference

Table 42: Program Management (PM)

Control (s)	Item	Response Data
PM-1	Does your organization have a Program Management policy (and subsequent procedures to facilitate the implementation of that policy) that addresses the purpose, scope, responsibility, management commitment, coordination among organizational entities, and compliance for all parties using CMS data? Is the policy disseminated to the appropriate personnel or roles? Is that policy reviewed and updated (as necessary) annually?	Yes or No
PM-2	Does your organization have a Chief Information Security Officer appointed to manage the security program, or similarly recognized official?	Yes or No
PM-12	Does your organization implement an insider threat program that includes a cross-discipline insider threat incident handling team?	Yes or No
PM-18	Does your organization develop and disseminate a strategic privacy plan?	Yes or No
PM-19	Does your organization have a Chief Privacy Officer appointed to manage the privacy program, or similarly recognized official?	Yes or No
PM-21	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?	Yes or No

If No 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.

Table 43: PM Rationale

Control (s) Referenced	Rationale
PM-	Rationale

Table 44: Personally Identifiable Information Processing and Transparency (PT)

Control (s)	Item	Response Data
PT-1	Does your organization have a Personally Identifiable Information Processing and Transparency policy (and subsequent procedures to facilitate the implementation of that policy) that addresses the purpose, scope, responsibility, management commitment, coordination among organizational entities, and compliance for all parties using CMS data? Is the policy disseminated to the appropriate personnel or roles? Is that policy reviewed and updated (as necessary) annually?	Yes or No
PT-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?	Yes or No
PT-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)?	Yes or No

If No 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.

Table 45: PT Rationale

Control (s) Referenced	Rationale
PT-	Rationale

Table 46: Supply Chain Risk Management (SR)

Control (s)	Item	Response Data
SR-1 SR-2	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?	Yes or No
SR-3 SR-6	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?	Yes or No

If No 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.

Table 47: SR Rationale

Control (s) Referenced	Rationale
SR-	Rationale

E. Overall Attestations and Audit Agreement

Please have the Data Custodian attest below. Please note, all related policies, procedures, and controls specified above may be subject to audit by CMS or CMS appointed personnel, including possible on-site engagements.

IMPORTANT: If required, this audit will be at the cost of the applicant.

Table 48: Attestation

Item	Response Data
Our environment is using a CSP, and we 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, identity & access management, etc.), while the CSP has responsibility for security “of” the cloud (compute, storage, networking, regions, availability zones, etc.).	Yes, No, or NA
I have reviewed all information, either presented above or attached to this review, and attest that is in fact true, complete, and accurate.	Yes or No
Name of QE	Name of QE
Name of Person Attesting	Name of Person Attesting
Title of Person Attesting	Title of Person Attesting
Date	MM/DD/YYYY