US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

03/27/2026

OPDIV:

CMS

Name:

Quality, Safety and Education Portal

PIA Unique Identifier:

P-4247073-827270

The subject of this PIA is which of the following?

Major Application

Identify the Enterprise Performance Lifecycle Phase of the system.

Operations and Maintenance

Is this a FISMA-Reportable system?

Yes

Does the system include a Website or online application available to and for the use of the general public?

Yes

Identify the operator.

Contractor

Is this a new or existing system?

Existing

Does the system have Security Authorization (SA)?

Yes

Indicate the following reason(s) for updating this PIA.

This system's authorization and PIA were previously approved through CCSQ's iQIES system. QSEP is being brought out from under the umbrella of iQIES to be its own, standalone system.

Describe in further detail any changes to the system that have occurred since the last PIA.

Surveyor Minimum Qualifications Test (SMQT): Transitioned this test from in-person mode on QSEP (implemented FY 2022)

Role requests, approvals, etc. have been moved to QSEP, from Savyint. This was completed by May 2024.

Contractor Surveyors: Contractor Surveyors are now required to complete the Surveyor Skills Review (SSR) assessments yearly starting with FY 2025. As part of this, a new role (Contractor Training Coordinator - CTC) has been added to QSEP.

Communications Platform: A new communications functionality - between CMS Quality, Safety, and Education Division (QSED) and State Directors - was introduced as part of the October 2024

release. A new role - State Director - was added to accomplish this.

Annual User Account Review: This was completed and went live in May 2023. As part of this, Security Officials (SO's) need to validate the accounts associated with their roles annually.

My Dashboard: a new landing page, displaying metrics associated with each role/user, was incrementally implemented during the FY 2024.

Training Initiation Form: This was migrated from Microsoft Forms to QSEP during FY 2023. This form is used by specific end users to notify CMS of any training changes.

NICE CXone Interactive Voice Response (IVR) for QSEP Help Desk was introduced during FY 2023.

Surveyor Skills Review (SSR): Emergency preparedness (EP) was included as secondary SSR and required to be completed by Surveyors undertaking EP survey.

Training Plan: Timelines were added to the Training plan to guide the users on completion timelines.

Describe the purpose of the system.

The Quality, Safety & Oversight Group (QSOG) provides Health Care Survey and Certification Processes training and course ware to more than 10,000 users nationwide, which includes State and Federal Surveyors, State Training Coordinators (STC), Regional Training Administrators (RTA), and Central Office Training Coordinators (TC). The Quality, Safety & Education Portal website (QSEP - https://qsep.cms.gov) is a cloud-hosted Learning Management System (LMS). The system is available 24x7. QSEP supports QSOG’s educational programs and provides administrative tools to effectively manage the National Surveyor Training Program (NSTP).

The main business function of QSEP is to deliver statutorily mandated training to State Agency and Federal surveyors, who provide survey and oversight to Medicare and Medicaid facilities around the country.

QSEP hosts more than 150 online courses, webinars, videos, and other instructional content that its users can access "anywhere at any time", using a web browser. The system is essential to QSOG's mandate to increase access to surveyor training by replacing most instructor-led "live" training with digital course content hosted and delivered online. QSEP provides site access to Healthcare Providers/Suppliers, Accrediting Organizations, Department of Health and Human Services (HHS) employees and contractors, Quality Improvement Organizations, Advocacy Groups, and the General Public.

Describe the type of information the system will collect, maintain (store), or share.

QSEP currently stores the following non-sensitive Personal Identifiable Information (PII) data elements:

student's first name

student's last name

student business telephone/fax numbers

student business email address (work, potentially home for self-registered users)

supervisor's first name

supervisor's last name

supervisor business telephone/fax numbers

supervisor business email address

The elements above are used only to identify users and enable reporting functionality within QSEP. Excluding students' first and last names, all data elements collected are considered non-sensitive. QSEP provides system functionality where users can update any PII related to their accounts. The QSEP Team attempts to always maintain a minimal dataset, following strict data retention policies mandated by HHS/CMS. In addition, the QSEP Team follows the Principle of Least Privilege for all user accounts and role-related system access.

No Protected health information (PHI) is stored within the system.

Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.

The Quality, Safety & Oversight Group (QSOG) provides Health Care Survey and Certification Processes training and course ware to more than 10,000 users nationwide, which include State and Federal Surveyors, State Training Coordinators (STC), Regional Training Administrators (RTA), and Central Office Training Coordinators (TC). The Quality, Safety & Education Portal website (QSEP - https://qsep.cms.gov) is a cloud-hosted Learning Management System (LMS). The system is available 24x7. QSEP supports QSOG's educational programs and provides administrative tools to effectively manage the National Surveyor Training Program (NSTP).

The elements captured in PIA-012 are used only to identify users and enable reporting functionality within QSEP. The information collected helps in tracking training and test/assessment completions, generate email notifications (for instance, to notify Regional Training Administrators (RTA) / State Training Coordinators (STC) on completion status of the assessments, and to notify the end user on the status of completions).

Does the system collect, maintain, use or share PII?

Yes

Indicate the type of PII that the system will collect or maintain.

Name
E-Mail Address
Phone Numbers

Indicate the categories of individuals about whom PII is collected, maintained or shared.

Employees
Business Partner/Contacts (Federal/state/local agencies)
Vendor/Suppliers/Contractors

How many individuals' PII is in the system?

100,000-999,999

For what primary purpose is the PII used?

The primary purpose of the PII used is to identify users and enable reporting functionality within QSEP. For instance, when a learner completes the training or assessment, a certificate is generated with the learner's name. CMS or Regional Training Administrators (RTA)/ State Training Coordinators (STC) run various reports to report on learner progress for Foundational Refresher

(FR) training, Surveyor Skills Review (SSR) assessment, to check on training progress against baselines, and to identify learners/surveyors who are currently inactive (have not logged in for 270+ days) to notify them to log in prior to the account being deactivated (365+ days since last login changes an account status to deactivated via automated scripts).

Describe the secondary uses for which the PII will be used.

Not applicable.

Identify legal authorities governing information use and disclosure specific to the system and program.

5 USC Section 301: Departmental Regulations

Are records on the system retrieved by one or more PII data elements?

No

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

Online

Government Sources

Within the OpDiv

State/Local/Tribal

Non-Governmental Sources

Public

Private Sector

Identify the OMB information collection approval number and expiration date

Not Applicable

Is the PII shared with other organizations?

No

Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.

Not applicable. QSEP receives the PII from HCQIS Access Roles and Permissions (HARP) as part of initial account creation. QSEP accounts are created and maintained in HARP, which serves as the secure identity management portal, QSEP users are redirected and authenticated against HARP.

Is the submission of PII by individuals voluntary or mandatory?

Voluntary

Describe the method for individuals to opt-out of the collection or use of their PII. If there is no option to object to the information collection, provide a reason.

There is no opt-out: PII is required for the creation of accounts in HARP and QSEP.

Process to notify and obtain consent from individuals whose PII is in the system when major changes occur to the system.

QSEP accounts are created and maintained in the HCQIS Access Roles and Permissions (HARP), which serves as CMS' Center for Clinical Standards and Quality (CCSQ) secure identity management portal. HARP is responsible for the process of notifying and obtaining consent from the individuals whose PII is in the system when major changes occur to the system. HARP is covered by a separate PIA.

Describe the process in place to resolve an individual's concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate.

As QSEP accounts are created and maintained in HARP, user' concerns are addressed by HARP. For details, see the QNet Enterprise Services Privacy Impact Assessment.

Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy.

QSEP accounts are created and maintained in the HCQIS Access and Role Permissions (HARP) which serves as the secure identity management portal. QSEP users are redirected and authenticated against HARP. When a QSEP user logs in to HARP and redirects to QSEP after successful login, PII data is validated with HARP, and if any changes, they are then updated in QSEP.

For Customer PII:
Integrity – Only the DevOps team has access to the database. Data updates done is tracked in the audit table, which is reviewed regularly to ensure the integrity of data. Users access QSEP via defined roles, which are reviewed and approved by Security Officials (SO) on role request creation and by the SO during the Annual Account Review (AAR) process. Splunk dashboard and scripts are reviewed by DevOps and the QSEP Security Analyst.

Availability – New Relic alerts notify the QSEP team on system availability. In addition, the QSEP Help Desk team notifies QSEP DevOps when performance degradation is observed.

Accuracy – Only the DevOps team has access to the database. Data updates are tracked in the audit table, which is reviewed regularly to ensure the integrity of data. Users access QSEP via defined roles, which are reviewed and approved by Security Officials (SO) on role request creation and by the SO during the Annual Account Review (AAR) process. Splunk dashboard and scripts are reviewed by DevOps and the QSEP Security Analyst. The QSEP team provides monthly data on multiple parameters to CMS to gauge the health and accuracy of the system.

Relevancy – The QSEP team reviews the audit table, runs scripts against Splunk to get statistics, provides various reports to CMS monthly provides monthly data on multiple parameters to CMS which ensure information is processed and delivered as expected. The QSEP Help Desk analyzes each help desk request.

For User PII:

Integrity – Every time that a user logs into QSEP via HCQIS Access Roles and Permissions (HARP), the user's PII data in QSEP is validated against HARP and if there are changes, the updates are applied to QSEP. Ony the QSEP DevOps team has access to the QSEP database. Actions performed on the database or undertaken via QSEP are audited via the QSEP audit table. Splunk QSEP dashboard provides a view into various logs to track DevOps activities.

Availability – New Relic alerts notify the QSEP team on system availability. In addition, the QSEP Help Desk team notifies QSEP DevOps when performance degradation is observed.

Accuracy – Every time that a user logs into QSEP via HCQIS Access Roles and Permissions (HARP), the user's PII data in QSEP is validated against HARP and if there are changes, the updates are applied to QSEP. Ony the QSEP DevOps team has access to the QSEP database. Actions performed on the database or undertaken via QSEP are audited via the QSEP audit table. Splunk QSEP dashboard provides a view into various logs to track DevOps activities.

Relevancy – QSEP maintains PII data that is needed for reporting and certificates. No other PII is maintained or collected via QSEP. Automated scripts are executed to ensure information is processed and delivered as expected.

Identify who will have access to the PII in the system and the reason why they require access.

Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.

Only the QSEP DevOps team has access to the production data. All QSEP users receive the least privilege necessary to perform their assigned job tasks. Users are only granted access based on their job responsibilities. To ensure the level of access is maintained for each of the roles, the role creation process involves analysis of the role definition and type of access granted by the role. Periodic account and access review ensures that system users are still authorized to view PII.

Describe the methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job.

QSEP users receive the least privilege necessary to perform their assigned job tasks. The QSEP user community is comprised of users with various roles that determine their access level. The Security Official (SO), who is responsible for verifying all accounts under their domain, review and approve/decline each role request. The SO verifies the user is granted roles that minimally meet their role description. These accounts are reviewed and validated at least once a year during the Annual Account Review process. The QSEP Security Official would be aware of any user changes within their area of responsibility. Accordingly, access to the system can be restricted/adjusted based on the business needs of the user at any time by the Security Official by going to the QSEP Learner Management module and adjusting the access/roles.

Identify training and awareness provided to personnel (system owners, managers, operators, contractors and/or program managers) using the system to make them aware of their responsibilities for protecting the information being collected and maintained.

All system and site administrator users are required to take an online Security Awareness Training and Identifying and Safeguarding Personally Identifiable Information Computer based training before they are granted user credentials. This training is required to be renewed annually for all existing users. All users are trained to perform the duties necessary to work within the system to perform their specific job functions.

Personnel with Security Significant Responsibility (SSR) such as developers, infrastructure/system administrators, database administrators, architects, security engineers, etc., also complete CMS Agency Role-Based Training (RBT) requirements on an annual basis, corresponding to the user's National Institute of Standards and Technology (NIST) National Initiative for Cybersecurity Education (NICE) role. Any new Application Development Organizational (ADO) users or existing ADO users with a new role complete RBST requirement within 60-days of beginning their new role.

Describe training system users receive (above and beyond general security and privacy awareness training).

The ADO (application developing organization) users complete onboarding training requirements. The ADO users also undertake personal training as part of their specific training target to maintain their technical knowledge. Additionally, CMS ISG (Centers for Medicare and Medicaid - Information Systems Group) throughout the year provide training that the ADO users can attend or request a training session.

Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?

Yes

Describe the process and guidelines in place with regard to the retention and destruction of PII.

CMS requires that learner records be retained by the system for 30-years from date of entry (NARA Disposition Authority: DAA-0440-2012-0006).

Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.

QSEP administrative controls include but are not limited to contingency plans and annual testing, backups of all files, offsite storage of backup files, background checks for all personnel, incident response procedures for timely response to security and privacy incidents, Initial security training with refresher courses annually, and annual role-based security training for personnel with assigned security roles and responsibilities.

Technical controls include but are not limited to user authentication with least privilege authorization, firewalls, Intrusion Detection and Prevention systems (IDS/IPS), encrypted communications, hardware configured with a deny all/except approach, auditing, and correlation of audit logs from all Systems.

Management controls include but are not limited to: Certification and Accreditation (C&A), annual security assessments, monthly management of outstanding corrective action plans, ongoing risk assessments, and automated continuous monitoring.

Identify the publicly-available URL:

https://qsep.cms.gov

Note: web address is a hyperlink.

Does the website have a posted privacy notice?

Yes

Is the privacy policy available in a machine-readable format?

Yes

Does the website use web measurement and customization technology?

Yes

Select the type of website measurement and customization technologies is in use and if it is used to collect PII.

Does the website have any information or pages directed at children uner the age of thirteen?

No

Does the website contain links to non- federal government websites external to HHS?

Yes

Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?

No