US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

04/10/2026

OPDIV:

CMS

Name:

Qualified Health Plan Enrollee Experience Survey

PIA Unique Identifier:

P-8271749-032873

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.

PIA Validation

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

No system changes.

Describe the purpose of the system.

The Qualified Health Plan (QHP) Enrollee Experience Survey (EES) exists in response to Section 1311(c)(4) of the Patient Protection and Affordable Care Act (PPACA). The Act requires the United States Department of Health and Human Services Secretary to develop an enrollee satisfaction survey system that assesses consumer experience with QHPs offered through a Health Insurance Exchange. It also requires a public display of information by each Marketplace to allow individuals to assess enrollee experience among comparable plans.

The goals of the survey are to provide comparable and useful information to consumers about the quality of health care services and enrollee experience with QHPs offered through the Exchanges, facilitate oversight of QHP issuer compliance with quality reporting standards, and provide actionable

information that QHP issuers can use to improve quality and performance. This webpage provides Vendor Applicants, Conditionally Approved Vendors, Approved Vendors, and Public Use File Users with a multipurpose interface to support survey data submissions.

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

The type of information to be collected and maintained includes:

Contact Us Page - Name, e-mail address

Vendor - vendor name, address, point of contact name, point of contact e-mail address, point of contact phone number, and username

System Administrators - User Account Name, Device Identifier (Internet Protocol (IP) address), and events logged.

The QHP website/application utilizes and inherits CMS' Identity Management (IDM) system for identity management and authentication for the protection of PII data. IDM is leveraged by CMS business applications used across CMS. Users of all business applications that integrate with IDM can use a single set of user credentials to access any integrated application. CMS IDM incorporates Multi-factor Authentication (MFA) into user authentication. MFA is an authentication method that requires the user to provide two or more verification factors to gain access to the QHP website/application. This includes the user providing account username, password and a six-digest code delivered by text message to a mobile device.

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

The Qualified Health Plan (QHP) Enrollee Experience Survey (EES) exists in a response to Section 1311(c)(4) of the Patient Protection and Affordable Care Act (PPACA) that requires the United States Department of Health and Human Services Secretary to develop an Enrollee Experience Survey system that assesses consumer experience with QHPs offered through a Health Insurance Exchange. It also requires public display of information by each Marketplace to allow individuals to assess enrollee experience among comparable plans.

As a condition of certification and participation in the Exchanges, CMS requires that QHP issuers submit QHP Enrollee Experience Survey response data and Quality Rating System (QRS) clinical measure data for their respective QHPs offered through an Exchange in accordance with CMS guidelines. Exchanges are also required to display QHP quality rating information on their respective websites.

The goals of the QRS and the QHP Enrollee Experience Survey are to:

Provide comparable and useful information to consumers about the quality of health care services and enrollee experience with QHPs offered through the Exchanges,

Facilitate oversight of QHP issuer compliance with quality reporting standards set forth in the PPACA and implementing regulations, and

Provide actionable information that QHP issuers can use to improve quality and performance.

The QHP Enrollee Experience Survey web application provides a centralized web site that will allow

QHP Issuers to attest to the survey eligibility criteria or report ineligibility status, includes details on how prospective survey vendors can apply to become an approved vendor and allows approved vendors the ability to login and submit survey data. It will also include functionality that will allow the QHP Enrollee Survey team to manage submissions and manage the meta data of the web application.

The QHP ESS web application has a user centric design and is architected using serverless technologies in Amazon Web Services (AWS).

The QHP website/application utilizes and inherits CMS' Identity Management (IDM) system for identity management and authentication for the protection of PII data. IDM is leveraged by CMS business applications used across CMS. Users of all business applications that integrate with IDM can use a single set of user credentials to access any integrated application. CMS IDM incorporates Multi-factor Authentication (MFA) into user authentication. MFA is an authentication method that requires the user to provide two or more verification factors to gain access to the QHP website/application. This includes the user providing account username, password and a six-digest code delivered by text message to a mobile device.

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
Mailing Address
Phone Numbers
Device Identifiers
User account name, password

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

Vendor/Suppliers/Contractors

How many individuals' PII is in the system?

100-499

For what primary purpose is the PII used?

The PII primary purpose is to authenticate Vendors accessing the website.

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

The secondary use of PII is to identify Vendors who use the system, and to be able to search Vendor records.

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

Authority for maintenance, collection and disclosure of information is given under sections 2719, 2723 and 2761 of the Public Health Service Act and section 1321(c) of the Affordable Care Act.

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

Yes

Identify the number and title of the Privacy Act System of Records Notice (SORN) that is being use to cover the system or identify if a SORN is being developed.

09-70-0560 Health Insurance Exchanges (HIX) Program

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

Online

Government Sources

Other

Non-Governmental Sources

Private Sector

Other

Identify the OMB information collection approval number and expiration date

OMB 0938-1221 expires 09/30/2026

Is the PII shared with other organizations?

Yes

Identify with whom the PII is shared or disclosed and for what purpose.

Describe any agreements in place that authorizes the information sharing or disclosure.

Not applicable. There are no agreements in place.

Describe the procedures for accounting for disclosures.

QHP EES does not collect PII from the general public. Vendors accessing the QHP EES website are presented with a "warning banner" when logging into the system providing consent once the banner is acknowledged by continuing to website.

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

QHP EES does not collect PII from the general public.

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.

QHP EES does not collect PII from the public. Vendors cannot opt-out of providing their names, address, e-mail address and usernames as this data is required to create their user accounts to access the system.

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

QHP EES does not collect PII from the public. Vendors would be notified by e-mail of any major changes or data use occurring to the system.

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.

QHP EES does not collect PII from the public. Vendors who believe their PII was obtained, used or disclosed inappropriately or incorrect can use the e-mail address on the website home page to contact QHP EES.

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

Processes for data integrity, availability, and accuracy are both automated and performed manually

by QHP EES database administrators. Periodic reviews of information collected in the system, including vendor PII, are performed at regular intervals. Data accuracy and relevancy are reviewed and validated by Data Quality Analyst on an ongoing basis as part of the work performed by QHP EES.

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.

The administrative procedures in place to determine which system users may access PII are authentication and authorization rules that give specific permissions to each role. The role-based access is based on the principle of "least privilege" where users are given 'need to know' and 'need to access' permissions. All user roles for the system are documented in the QHP EES System Security Plan.

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.

The system controls in place for access to PII include role-based access permissions, and limits on the PII that is displayed so that only the minimum amount of PII is visible to users. Users are assigned different roles corresponding to different levels of access to data as well as the ability to perform specific actions (e.g., read, update, delete).

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 QHP EES personnel undergo corporate and project-specific training at time of hire and annually thereafter. This training includes security and privacy awareness training with content specifically to the protection of PII. QHP EES personnel must also complete project-specific training before starting work on the project or receiving access to additional roles within QHP EES. In addition, all personnel must sign agreements to acknowledge awareness of their responsibilities to protect this information.

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

QHP EES personnel must complete additional project-specific training before starting work on the project. Training courses provided by the agency or contractor include content about correct use of QHP EES as well as how to conduct case analysis and other project activities performed using the system

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.

PII within QHP EES is maintained as long as needed to support providing information to consumers about the quality of health care services and enrollee experience the Health Insurance Exchanges.

QHP operates in accordance with National Archives and Records Administration (NARA) General Records Schedule DAA-GRS-2013-0002.

As required by regulation, HHS must ask NARA for a variance when not following the retention

periods outlined by these schedules (36 CFR 1228.40(c)).

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

PII is secured in the system using administrative, technical, and physical controls, in accordance with policies and regulations detailed in the CMS Information Security Acceptable Risk Safeguards-Minimum Security
Requirements (ARS).

Administrative controls include role-based permissions to access Center for Consumer Information and Oversight (CCIIO) Customer Relations Management System (CCRMS) web pages and applications, request and authentication through the CMS Enterprise Identity Management (EIDM) system, periodic review of users and deletion of non-active accounts, security and network policies and procedures as well as security and privacy training regarding securing PII.

Technical controls include role-based access, inactivity timeout, multi-factor authentication. data encrypted at rest, data encrypted while being transmitted electronically, network firewall, anti-virus/malware prevention, intrusion detection/prevention technologies, centralized event log monitoring and event alerts. CCRMS, being hosted in the cloud inherit physical security controls from the Federal Risk and Authorization Management Program (FedRAMP) Salesforce Cloud and Amazon Web Services Cloud.

Identify the publicly-available URL:

https://qhpsurvey.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?

No

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?

No

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

null