US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

05/20/2016

OPDIV:

CMS

Name:

End Stage Renal Disease Quality Incentive Program

PIA Unique Identifier:

P-1675897-216612

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?

No

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 major system changes since last PIA

Describe the purpose of the system.

The purpose of the End-stage Renal Disease Quality Incentive Program (ESRD QIP) is to be the nation's first pay-for-performance (also known as "value-based purchasing") quality incentive program as mandated by the Medicare Improvements for Patients and Providers Act of 2008 (MIPPA) section 153(c). This first-of-its-kind program provides the ESRD community with the opportunity to enhance the overall quality of care that ESRD patients receive as they battle this disease. The ESRD QIP is the most recent step in fostering improved patient outcomes by establishing incentives for dialysis facilities to meet or exceed performance standards established by CMS. This step has been an important component of the Medicare ESRD payment system

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

ESRD QIP collects, maintains, and shares the following types of information in support of ESRD patients and their treatment:

Patient Information: Patient Social Security Number (SSN), Name, Date of Birth, Email Address, Phone Numbers, Medical Notes, Medical Records Number, Mailing Address, Employment Status, Gender, Date of Death (if applicable), Race/Ethnicity, and Health Insurance Claim Number (HICN).

Facility Information: Facility Name, Facility Address, Region, Facility Type.

Facility Personnel Information: Name, E-mail, Phone Number, and Position.

The user communities and stakeholders for these applications include CMS, ESRD networks, dialysis facilities, Medicare Secondary Payers (MSPs), Large Dialysis Organizations (LDOs), Batch Submitting Organizations (BSOs), the National Renal Administrators Association (NRAA), and the Social Security Administration (SSA). CMS federal direct contractors also have access to ESRD QIP in support of their contractual roles as administrators and developers. All users access ESRD QIP by logging into the QualityNet Secure Portal (QSP) and then selecting the ESRD QIP application. To login to the QSP, users must first submit a user account application to the QualityNet Help Desk. Once the account has been reviewed and approved, the user credentials (username, password, email) are stored in the QualityNet Enterprise Service (QNet ES) system which provides the access for the QSP. User credentials contain PII. User credentials are stored temporarily within QNet ES in accordance with the Center for Clinical Standards and Quality (CCSQ) Records Schedule and File Plan. QNet ES is a separately accredited system with its own PIA.

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

ESRD QIP receives patient, claims and facility data for the purpose of calculating facility performance scores. Information is received, maintained, and shared temporarily by ESRD QIP and follows the CMS CCSQ Records Schedule and File Plan which adheres to the National Archives and Records Administration (NARA) guidelines.

User credentials are used to access the system and are stored temporarily within QNet ES in accordance with the CCSQ Records Schedule and File Plan

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

Yes

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

Social Security Number

Date of Birth

Name

E-Mail Address

Mailing Address

Phone Numbers

Medical Records Number

Medical Notes

Employment Status

Other - Gender, Race/Ethnicity, Health Insurance Claim Number (HICN), Date of Death

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

Patients

How many individuals' PII is in the system?

10,000-49,999

For what primary purpose is the PII used?

The PII collected by ESRD QIP is all patient specific and is used to uniquely identify a patient and properly associate patient records with an individual. User Credential PII is collected via CMS' Enterprise Identity Management (EIDM) account registration and is used to access the system to support operations.

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

Not Applicable

Describe the function of the SSN.

The Social Security Number is used to uniquely identify a patient and properly associate patient records with an individual.

Cite the legal authority to use the SSN.

The Social Security Act (42 USC 405 (c)(2)(F)) requires a Social Security beneficiary to provide his or her SSN as a condition for receipt of benefits under Title II of the Social Security Act, Medicare eligibility due to end stage renal disease (ESRD).

The statutory authority for this system is given under the provisions of Sections 226A, 1875, and 1881 of the Social Security Act (the Act) (Title 42 United States Code (U.S.C.), sections 426–1, 1395ll, and 1395rr).

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

End-stage Renal Disease Quality Incentive Program (ESRD QIP) is mandated by the Medicare Improvements for Patients and Providers Act of 2008 (MIPPA) section 153(c).

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.

09-70-0520 , ESRD Program Management and Medical Information System

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Government Sources

Within OpDiv

Other HHS OpDiv

Non-Governmental Sources

Private Sector

Identify the OMB information collection approval number and expiration date

No OMB information collection approval is required because PII in ESRD QIP is not received directly from the individuals with whom the information pertains.

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.

Patients are given an informed consent form stating the uses of their PII from the dialysis clinic.

ESRD QIP system end-users are given Terms and Conditions during the EIDM account registration process which include Consent to Monitoring, Protecting Your Privacy, and Consent to Collection of Personal Identifiable Information (PII). Users will be emailed at the email address provided during registration if there are any changes in the Terms and Conditions.

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 option to object to the information collection, patient PII is required for Medicare eligibility and claims processing.

End-users cannot object to providing PII during EIDM account registration as it is needed to properly verify user identity and create the account.

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

Individuals are directly notified of major changes to the system via their respective Dialysis Facility. The CMS Quality Improvement Group (QIG) communicates to the End Stage Renal Disease (ESRD) Networks, who then communicate to the Dialysis Facilities. The Dialysis Facilities have the direct relationship with the individuals.

System Users will be emailed at the email address provided during EIDM account registration if there are any changes in the Terms and Conditions with regard to how their PII is being used.

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.

Patients with concerns about PII collection and disclosure are referred to the patient's dialysis clinic. If the clinic is not able to assist the individual directly, they will raise the issue to the Quality Net Enterprise Service Desk by issuing a ticket. The Quality Net Enterprise Service Desk will triage the issue and resolve appropriately.

System user's credential information is collected via registration with CMS Enterprise Identity Management (EIDM), therefore, no process exists for ESRD QIP. The issue should be reported to the CMS IT Service Desk and escalated to the EIDM administrators.

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

ESRD QIP PII is validated based on input from the Dialysis Facilities, ESRD Networks and CMS Administrative users who perform reconciliation of the eligibility information on an ongoing basis.

EIDM and QNet ES perform their own account auditing to review the user credentials containing PII.

Audits include controls such as bi-annual reviews of account information accuracy, verifications of account need, disabling accounts after periods of inactivity, and immediate revocations of access for users leaving CMS contracts.

All systems follow a subset of the CMS Acceptable Risk Safeguard (ARS) 2.0 controls focus on PII and ensuring its confidentiality, integrity, and availability.

Modifications to system data are logged and can be attributed specifically to the user doing the modifications via their CMS enterprise credentials. If PII is somehow accidentally or intentionally destroyed by a user responsible for that PII, it can be restored from backup. The program has developed availability metrics with corresponding technical solutions to ensure data is accessible when necessary. Contingency planning and disaster recovery tests are also performed annually for the systems to ensure that data recovery is effective and timely.

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

Users:

Analytic user - to perform patient-level data analysis. This user base is very limited; approximately 5 Full Time Employee (FTE).

Administrators:

Database administrators and production control personnel have access in order to maintain the system and create the exports of the information from the system as necessary. These users are direct contractors but have the proper roles, have undergone background checks, and have taken required training.

Contractors:

Direct contractor database and systems administrators do have access to the PII for the purpose of troubleshooting and maintaining the system. These users are defined on an access roster, have the proper roles, have undergone background checks, and have taken required training.

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

All users of the system have access to PII, the extent of which depends on their system role. All users are vetted through CMS' Enterprise Identity Management (EIDM) website to apply for, obtain approval and receive a user ID that can be used to access the application. A users must register through EIDM for a user ID and password. Requests go to the CMS Identity Management team where they will review the validity of the request and the accuracy of the information provided. Once the user has received a val ID user id and password a request must be made for access to an application and role. The approvers will review the request and justification and either approve, reject or defer. These procedures are documented in the CMS Enterprise Identity Management (EIDM) User Guide.

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.

Users are assigned to roles within EIDM designed to give the least privilege required to perform their job/contracted role. Access to roles requested and approved through EIDM.

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 users are required to take the CMS Cyber Awareness Challenge Computer Based Training (CBT) as well as the Identifying and Safeguarding Personally Identifiable Information (PII) training endorsed by CMS.

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

Security and Privacy Awareness training is offered through Computer Based Training to all users.

Training is required for acquire and hold an EIDM account (used for ESRD QIP authentication). EIDM is responsible for enforcing current, up-to-date training. Contractors that have elevated levels of access, such as system or database administrators, have to take additional role- based training as required within the CMS Acceptable Risk Safeguards (ARS) 2.0 controls for security.

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.

ESRD QIP follows the CMS Record Schedule, more specifically the Center for Clinical Standards and Quality (CCSQ) File Plan. This is inherited from the National Archives and Records Administration (NARA). NARA has recently made changed to has made to Federal Advisory Committee Act (FACA), Freedom of Information Act (FOIA), Information Technology (IT), transitory files, travel, Records management, forms management and Contract Officer Representative (COR) information and responsibilities. The disposal authority for ESRD QIP is N1-440-09-3 and calls for destruction of data after 10 years.

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

ESRD QIP PII is secured with a variety of security controls as required by FISMA and the CMS Security Program. Operational controls include but are not limited to: contingency plans and annual testing, backups of all files, offsite storage of backup files, physical security including secure buildings with access cards for entry, secure data center requiring additional access permissions for entry, security guards, 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), hardware configured with the National Institute of Standards and Technology (NIST) security checklists, 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.