# US Department of Health and Human Services

## Privacy Impact Assessment

### Date Signed:

05/16/2016

### OPDIV:

CMS

### Name:

Consolidated Renal Operations in a Web-Enabled Environment

**PIA Unique Identifier:**

P-5298886-371690

**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?**

New

**Does the system have Security Authorization (SA)?**

Yes

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

**Describe the purpose of the system.**

The CMS Center of Clinical Standards and Quality's (CCSQ) Consolidated Renal Operations in a Web-Enabled Environment (CROWN) system is a CMS Major Application (MA) which facilitates the collection and maintenance of information about the Medicare End Stage Renal Disease (ESRD) program; including ESRD beneficiaries/ patients, Medicare approved hospitals and dialysis facilities, and Department of Veterans Affairs (DVA) ESRD patients.

CROWN also provides CMS the tools needed to measure and improve the efficacy of CMS’s renal medicine program. CROWN determines the Medicare coverage periods for ESRD patients and serves as the primary mechanism to store and access information in the ESRD Program Management and Medical Information System Database (PMMIS). Additionally, CROWN tracks the ESRD patient population for both Medicare and non-Medicare patients.

The primary goals of CROWN for CMS are to eliminate ESRD information collection redundancy; improve data accessibility; improve the lives of individuals with ESRD; promote quality improvement

in the program; provide more timely data to CMS; provide value to the dialysis community; and strengthen ESRD community collaboration.

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

The following information is collected, maintained and shared by CROWN: ESRD patient personal information, patient treatment information, treatment facility information, and treatment facility personnel information.

ESRD patient personal information includes: patient Social Security number (SSN), name, date of birth, mailing address, telephone number, medical notes and medical record information, employment status, gender, race/ethnicity, date of death (if applicable) and Health Insurance Claim Number (HICN)/ Medicare claim number.

Patient treatment information includes: medical information, lab results, prescription history and dialysis history and provider information (name, address, telephone number).

Facility information includes: name, location, type of facility, services provided, number and type of medical staff, patient statistics (number and type of treatment) and facility personnel information (name, facility email and phone number, and position).

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

The CROWN system collects and maintains information about the Medicare ESRD program, its beneficiaries, facilities and services provided to beneficiaries.

It also provides CMS the information needed to measure and improve the efficacy of CMS's renal medicine program. The primary goals of CROWN for CMS are to eliminate ESRD information collection redundancy; improve data accessibility; improve the lives of individuals with ESRD; promote quality improvement in the program; provide more timely data to CMS; provide value to the dialysis community; and strengthen ESRD community collaboration.

CROWN provides the following capabilities: a single system for all users to collect, submit, and report ESRD data; an environment to manage timely and accurate ESRD data to provide for better quality care; and a single system with electronic communications between CMS, ESRD networks and dialysis facilities.

The following information is collected, maintained and shared by CROWN for the length of time necessary for reporting, evaluation and as required to manage the ESRD program. The ESRD information stored is ESRD patient personal information, patient treatment information, treatment facility information, and treatment facility personnel information. The information is captured on three CMS forms: CMS 2728-U3 ESRD Medicare Entitlement and Patient Registration; CMS Form 2746 ESRD Death Notification; and CMS Form 2744 ESRD Facility Survey.

ESRD patient personal information includes: patient SSN, name, date of birth, mailing address, telephone number, medical notes and medical record information, employment status, gender, race/ethnicity, date of death (if applicable) and Health Insurance Claim Number (HICN)/Medicare claim number.

Patient treatment information includes medical information, lab results, prescription history and dialysis history and provider information (name, address, telephone number).

Facility information includes: name, location, type of facility, services provided, number and type of medical staff, patient statistics (number and type of treatment) and facility personnel information (name, facility email and telephone number, and position).

CROWN system access is through the QualityNet Enterprise Service (QNet ES) Secure Portal (QSP). To access CROWN, a user (both external and internal CMS users) logs into QSP and then selects the CROWN application. The user credentials (user ID and password) are collected and maintained by the QNet ES system which has its own separate PIA to address the information contained within QNet ES.

CROWN users include registered and approved individuals from the following organizations: CMS (employees and direct contractors), ESRD networks, dialysis facilities, Medicare Secondary Payers (MSPs), Large Dialysis Organizations (LDOs), Batch Submitting Organizations (BSOs), and the National Renal Administrators Association (NRAA).

**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 - Date of Death, Race/Ethnicity, Gender, Health Insurance Claim Number (HICN); job position.

SSN is used to uniquely identify a patient.

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

Patients

ESRD network and dialysis facility personnel

**How many individuals' PII is in the system?**

10,000-49,999

**For what primary purpose is the PII used?**

The PII collected is used to enroll a person in the ESRD program and track their participation and provide information to CMS for program review and maintenance.

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

Not Applicable

**Describe the function of the SSN.**

The SSN is used to uniquely identify a patient and determine eligibility to receive Medicare benefits. It is only disclosed/shared between CMS and the SSA.

**Cite the legal authority to use the SSN.**

Executive Order 9397 and Sections 226A, 1875 and 1881 of the Social Security Act; Title 42 U.S.C., sections 426-1, 1395ll and 1395rr

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

Code of Federal Regulations (CFR) 42 Section 494.180(h) and
Sections 226A, 1875 and 1881 of the Social Security Act; Title 42 U.S.C., sections 426-1, 1395ll and 1395rr

**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 (PMMIS) published

**Identify the sources of PII in the system.**

Online

**Government Sources**

Within OpDiv

Other Federal Entities

**Non-Governmental Sources**

Private Sector

**Identify the OMB information collection approval number and expiration date**

OMB 0938-0447 - approved 2/14/14 and expires 12/31/16
OMB 0938-0046 - approved 7/14/14 and expires 04/30/2017
OMB 0938-0448 - approved 8/6/14 and expires 04/30/2017

**Is the PII shared with other organizations?**

Yes

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

**Other Federal Agencies**

The Social Security Administration receives SSN information from CROWN regarding the enrollment in and cessation of ESRD coverage to determine potential entitlement and elimination of Medicare coverage.

**Private Sector**

The CROWN system shares PII with the University of Michigan Kidney Epidemiology and Cost Center (UM-KECC). On a monthly basis, an extract of all facilities, patients, admit/discharge/treatment data, and clinical data is placed in an export file, encrypted and burned to a CD, and securely delivered to UM-KECC. UM-KECC compiles the clinical data to generate Clinical Performance Measures (CPM) about the facilities and the CPM are sent back to CROWN for use in reporting.

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

CMS has a Computer Matching Agreement (CMA) with SSA for the sharing of PII/SSN between the Departments.

An MOU is in place between CROWN and the Health Care Quality Improvement System (HCQIS) data center.

There is an ISA in place between CROWN and UM-KECC to authorize the data extracts that they receive.

**Describe the procedures for accounting for disclosures.**

There are no disclosures of PII outside what is permissible for CROWN to provide its functions and purpose for CMS. The system accounts for disclosures through formally established CMS Data Use Agreements (DUAs) between CMS and its CROWN stakeholders. The DUA details the data which CROWN stakeholders are privileged to access and conditions for use of
the data.

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

The collection of personal information is done at the ESRD facility level and not directly by CROWN. At the ESRD facility, patients are given an informed consent form stating the uses of their PII.

**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.**

The collection of PII is done at the ESRD facility level and not directly by CROWN, so there is no option to opt-out of the collection of PII, for patients in the ESRD program. A patient's PII is required for Medicare ESRD eligibility and claims processing.

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

The collection of PII is done at the ESRD facility level and not directly by CROWN. The CROWN system does not directly notify ESRD patients. The CCSQ, the CMS component that CROWN operates under, would issue a memo to the ESRD community, and then the ESRD facilities would notify their patients.

**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.**

Any individuals with concerns about their PII collection and disclosure would contact the ESRD facility or dialysis clinic where they receive care. That facility would contact CMS to determine if there were any next steps that would need to take place.

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

The PII within CROWN is validated for integrity, availability, accuracy and relevancy by the input from the dialysis facilities and ESRD networks. Any incorrect data is corrected in the course of using the system by updating whichever element is incorrect, such as a name change or new telephone number or email address. CMS administrators, who have access to PII, perform reconciliation of the eligibility information on an ongoing basis.

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

**Users:**

The dialysis clinic and ESRD Network users of the system have access to the PII in the system to register, handle patient billing, and maintain patient records in CROWN. CMS users have access to data for all facilities and ESRD Networks.

**Administrators:**

Database administrators and database personnel may have access in order to maintain the system and create the exports of the information from the system as necessary. System administrators would not have access to PII except on a limited, by exception basis.

**Contractors:**

Direct contractors, in their roles as database and systems administrators, may have access to the PII for the purpose of troubleshooting and maintaining the system and creating export data.

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

The procedures to determine system access and access to PII is done by job code assigned by CMS' Enterprise Identity Management system (EIDM). CROWN users must register through EIDM for a user ID and password. After the individual is approved for a user ID, the person must request access to CROWN and is assigned a role which determines the amount and what type of information that is accessible and visible to the user.

**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. Direct contractor accounts are reviewed annually in order to determine if a user still requires access to the system.

**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 CMS employees and direct contractors with access to CMS networks, applications, or data must complete mandatory annual Privacy Awareness Training annually. All CROWN users are required to take the CMS Cyber Awareness Challenge, and the Identifying and Safeguarding Personally Identifiable Information (PII) training.

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

CMS employees and contractors with elevated levels of access, such as system or database administrators, have to take additional role- based training as required.

**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.**

CROWN follows the CMS Record Schedule, published April 2015 under the Health Care Quality Improvement Systems (HCQIS) section XIV, Item P. The disposition authority for CROWN 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.**

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

The physical security of the data center where the system resides includes the use of access cards for entry, security guards, and video monitoring.

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.