# US Department of Health and Human Services

## Privacy Impact Assessment

### Date Signed:

06/09/2025

### OPDIV:

NIH

### Name:

NIDDK GSS United States Renal Data System (USRDS)

**PIA Unique Identifier:**

P-1180780-129659

**The subject of this PIA is which of the following?**

Minor Application (child)

**Identify the Enterprise Performance Lifecycle Phase of the system.**

Operations and Maintenance

**Is this a FISMA-Reportable system?**

No

**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.**

The security authorization date and the specific records retention schedules have been updated.

**Describe the purpose of the system.**

The United States Renal Data System (USRDS) is a national data system that collects, analyzes, and distributes information about chronic kidney disease (CKD) and end-stage renal disease (ESRD) in the United States (US), including treatments and outcomes. The USRDS is funded by the National Institutes of Health (NIH), National Institute of Diabetes and Digestive and Kidney Diseases (NIDDK).

The USRDS has six goals: (1) to characterize the ESRD population; (2) to describe the prevalence and incidence of ESRD, along with trends in mortality and disease rates; (3) to investigate relationships among patient demographics, treatment modalities, and morbidity; (4) to report the costs of ESRD treatments and total burden of ESRD program in the US; (5) to identify new areas for

special renal studies and support investigator-initiated research; and (6) to provide data sets and samples of national data to support research studies.

Along with producing the Annual Data Report (ADR) on ESRD and CKD in the US, the USRDS also fulfills data requests; provides standard analysis files (SAF) and specialized datasets to researchers; produces a Researcher's Guide to the USRDS; and presents the results of its research at national conferences and in peer-reviewed journals.

USRDS staff collaborate with members of the Centers for Medicare and Medicaid Services (CMS), the United Network for Organ Sharing (UNOS), and the ESRD Network group, sharing datasets and actively working to improve the accuracy of ESRD patient information. The USRDS Coordinating Center is operated by the Chronic Disease Research Group (a division of Hennepin Healthcare Research Institute located in Minneapolis, Minnesota) who is contracted by NIDDK.

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

The USRDS collects and analyzes information received from the Centers for Medicare and Medicaid Services (CMS) regarding patients with CKD and ESRD in the United States.

To identify individuals, USRDS stores Name, Social Security Number (SSN), Phone Number, Medical Records Number, Date of Birth, and Patient Identifiers [Consolidated Renal Operations in a Web-enabled Network (CROWNWeb) identification (ID), Standard Information Management System (SIMS) ID, and Renal Management Information System (REMIS) ID]. Billing information is collected to track incidence and prevalence of certain disease conditions. Zip code, high-level insurance information (i.e. Medicare primary or secondary, Health Maintenance Organization (HMO) or Preferred Provider Organization (PPO), Employer-provided, etc.), CMS Beneficiary ID, and medical claim numbers are also collected. Finally, employment status is collected to help analyze whether a patient's health is optimal enough to be employable. The information is aggregated when shared.

The USRDS uses specific login information for researchers to query public domain data from USRDS. Login account creation requires name, organization, email address, and password which serves as the login name.

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

The USRDS collects and analyzes information received from the Centers for Medicare and Medicaid Services (CMS) regarding patients with CKD and ESRD in the United States.

To identify individuals, USRDS stores Name, Social Security Number, Phone Number, Medical Records Number, Date of Birth, and Patient Identifiers [Consolidated Renal Operations in a Web-enabled Network (CROWNWeb) identification (ID), Standard Information Management System (SIMS) ID, and Renal Management Information System (REMIS) ID]. Billing information is collected to track incidence and prevalence of certain disease conditions. Zip code, high-level insurance information (i.e. Medicare primary or secondary, Health Maintenance Organization (HMO) or Preferred Provider Organization (PPO), Employer-provided, etc.), CMS Beneficiary ID, and medical claim numbers are also collected. Finally, employment status is collected to help analyze whether a patient's health is optimal enough to be employable. The information is aggregated when shared.

The USRDS uses specific login information for researchers to query public domain data from USRDS. Login account creation requires name, organization, email address, and password which serves as the login name.

**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
Phone Numbers
Medical Records Number
Employment Status
Patient Identifiers (ID): Consolidated Renal Operations in a Web-enabled Network (CROWNWeb) ID, Standard Information Management System (SIMS) ID, Renal Management Information System (REMIS) ID
Medical Claim Number(s), Billing information, CMS beneficiary identification number, medical insurance information, zip code
User login information, organization, password

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

Public Citizens
Patients

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

1,000,000 or more

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

To complete the USRDS Annual Data Report.

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

To share USRDS data with researchers as limited datasets which will not include primary PII such as name, address, identification number, social security numbers, and health insurance identification numbers.

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

42 U.S.C. 241a, 289c, as last amended by Public Law 100-607, November 4, 1988 under the Health Omnibus Programs Extension of 1988.

**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.**

SORN 09-25-0160 United States Renal Data System

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

Government Sources
Other HHS OpDiv
Non-Governmental Sources
Identi

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

Public Law 114-255, Section 2035, exempts research conducted by NIH from Paperwork Reduction Act (PRA) requirements.

**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.**

There is an Information Exchange Agreement (IEA) in development between NIDDK and CMS. There is also an Interagency Agreement (IAA) between NIDDK and CMS. USRDS requires a signed Data Use Agreement (DUA) from outside researchers outlining roles, responsibilities, and terms for data use and any disclosures as part of the data request process.

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

To request data from the USRDS, a researcher must submit three documents: (1) properly formatted research proposal (2) memo indicating Institutional Review Board (IRB) approval or exemption of the project, (3) signed Data Use Agreement. NIDDK maintains a spreadsheet of all approved requests, including the submitted documents.

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

Prior to any treatment and collection of medical data, the patient signs CMS Protocol Consent Form 2728. By consenting to medical treatment, the patient is implicitly acknowledging the collection of medical data. The protocol consent form explicitly addresses the use and distribution of that data with respect to confidentiality and the Privacy Act.

**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.**

Patients can elect not to complete CMS Form 2728, but that would preclude them from the study.

Researchers can elect not to provide PII and sign the Data Use Agreement form, but that would preclude from accessing USRDS or making a data request from the system.

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

If there are any changes in the study/protocol regarding data policy or data usage, patients are required to sign any newly approved amendments to the consent.

**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.**

Individuals may write to the System Manager, U.S. Renal Data System, Coordinating Center (CC), 914 South 8th Street, Suite D-206, Minneapolis, MN 55404.

Concerned individuals must provide notarized signature as proof of identity, and their request should include as much of the following information as possible: (a) Full Name, (b) Title of project that individual participated in, (c) Approximate dates of participation, (d) Description of the record contents being sought/contested (e) Description of the corrective action sought with supporting information to show how the record is inaccurate, incomplete, untimely (obsolete), or irrelevant (if applicable).

Individuals may also request listings of accountable disclosures that have been made of their records, if any.

**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 USRDS Coordinating Center (NIDDK contractor) performs audits and validations of data sources at least annually. They compare current data with the original files received from CMS.

**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.**

Determinations are made based on role-based access controls and least privilege. User rights are provisioned based on controls within the system, allowing users only access to the minimum amount of PII necessary to perform their job.

**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.**

Access to PII is assigned to personnel based upon current job responsibilities.

**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.**

According to NIH policy, all personnel who manage or operate NIH applications must successfully complete annual security awareness training. Training is completed on the http://irtsectraining.nih.gov site with valid NIH credentials.

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

Administrators and Privileged Users require additional training specific to their roles and responsibilities.

**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.**

Item 02-001 - Official Case Files of Construction, Renovation, Endowment and Similar Grants
These records encompass documents for managing and monitoring grand-supported research facilities. They include total application, progress reports, site visits, summary of review actions, award notices, terms and conditions of award, financial status reports, close-out documents, and

other related papers maintained as an identifiable entity to be used in monitoring the use of supported space throughout the usage obligation.
Disposition: Cut off annually following completion of final grant-related activity that signifies closing of the case file (e.g., project period ended). Destroy 20 years after cutoff. DAA-0443-2013-0004-0001

Item 02-004 - Extramural Program and Grants Management Oversight Records
These records are generated during the administration and execution of extramural program activities. They include the following extramural functions and operations: grant award administration, stakeholder liaison, human subjects protection, intellectual property, peer review, data management and reporting, research integrity, communication and outreach.
Disposition: Cut off annually. Destroy 3 years after cutoff. DAA-0443-2013-0004-0004

Item 02-005 - Official Case Files of Applications and Awards, Appeals, and Litigation Records for Grants, Cooperative Agreements, and Other Transaction Activities
These records include the complete application(s), summary of review actions, award notices, progress reports, financial records, audit records, official correspondence, appeal documents, legal opinions and litigation documents, closeout documents, and all other related significant and supporting documents that pertain only to the particular grant and grant owner(s).
Disposition: Cut off annually following completion of final award-related activity that represents closing of the case file (e.g., end of project period, completed final peer review, litigation or appeal proceedings concluded). Destroy 30 year(s) after cutoff. DAA-0443-2019-0008-0001

Item 03-005 – Patient Medical Records
These records document admissions and medical treatment for a patient accepted in a research project. These records are the primary source of evaluation and analysis for either clinical care or clinical research study.
Disposition: Cut off annually after medical staff member leaves patient care. Transfer to inactive storage 1 year after cutoff. Destroy 30 years after cutoff. DAA-0443-2012-0007-0011

Item 03-006 – Medical Staff Credentialing Records
These records are comprised of X-rays and other roentgenographic images produced by devices and procedures, such as body/head scans created by computerized transaxial tomography (CT). Files may include physician interpretations of images/scans.
Disposition: Cut off annually after medical staff member leaves patient care. Transfer to inactive storage 1 year after cutoff. Destroy 30 years after cutoff. DAA-0443-2012-0007-0007

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

Physical Controls: The IT hardware used to host protected information is located in a secured data center facility. The facility is only open to authorized personnel whose access is monitored by locking doors with badge readers for both ingress and egress. Each discrete ingress and egress event is logged. The facility is under 24-hour surveillance by facilities security for security and environmental hazards. Data tapes and hard copy data files are stored and locked in secured areas. Fire alarms and extinguishers are located in computer/data storage rooms. Offices are monitored for temperature and water/humidity.

Technical Controls: IT hardware and software is segregated from default commodity public networks to prevent unauthorized or malicious access. Access controls lists and event logs are maintained and monitored to detect unauthorized, suspicious or malicious activity. Access lists are restricted to

approved IT technical personnel.  Data is backed up, and a contingency plan is in place in order to plan for the disruption of services.

Administrative Controls: All technical personnel who access IT systems which contain protected information have met background investigation criteria, certifications, and requirements for their duties. All personnel have taken mandatory security and privacy training classes and annual refreshers. A framework of policies and procedures for day-to-day operations of the system and component applications has been established. Privileged access is limited to specific positions/roles.

**Identify the publicly-available URL:**

www.usrds.org

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?**

Yes