US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

05/06/2026

OPDIV:

CMS

Name:

CCSQ Data Repository and Analytics Platform

PIA Unique Identifier:

P-3503590-335823

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.

Agency

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

Significant System Management Change

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

Modifications to system, ports, protocols, or services

Installation of new or upgraded system specific support software, middleware component, application or cloud service

New User Roles Added

Installation of a new or upgraded middleware component or application.

New connection to data source and Application Programming Interface (API)

Modifications on how information, including personally identifiable information/protected health information (PII/PHI), is processed, stored, and/or transmitted

New connection to Short Message Service (SMS) ATO'd FISMA system or Service

Infrastructure code changes

New environment: Migration to Cloud, Pre-Production, etc.

New or updated cloud/non-cloud Servers, Communication Devices, or database

Change in Operating System

Feedback Analysis System (FAS) was removed from the Center for Clinical Standards and Quality (CCSQ) Data Repository and Analytics Platform (CDRAP) Authorization to Operate (ATO) boundary to become its own FISMA system

Describe the purpose of the system.

CDRAP: The Center for Clinical Standards and Quality (CCSQ) Data Repository and Analytics Platform (CDRAP) supports the QualityNet Data & Modernization Project's requirement to establish a cloud-based centralized data repository (CDR) in the QualityNet cloud environment and internet-facing multi-tool analytic solution, The CDR provides convenient, secure, and more timely access to CCSQ Quality data and commonly used datasets sourced from CMS systems of record. CDRAP functionality includes data wrangling, data visualization, basic statistics, and advanced modeling capabilities.

STAR: Strategy for Analytics & Reporting (STAR) is tasked with developing a set of best-practices, standards, and reusable software components that should be applied/utilized within Center for Clinical Standards and Quality (CCSQ) lines of business (LOBs) to ensure that their future efforts are aligned with the "One CCSQ" vision. This includes a scalable, iterative, and incremental process for collaboration among LOBs through a centralized CCSQ Amazon Web Services (AWS) Redshift data warehouse instance that also has access to all centralized data repository (CDR) data sources.

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

CDRAP: CCSQ Data Repository and Analytics Platform (CDRAP) does not collect new data. CDRAP uses copied datasets from existing data analytics systems. A copy of the original data for all types of PII/PHI that exist in consuming LoBs (Line of Business). The copied data is kept within CDRAP and can be dropped when it is no longer needed. The collected copied data for LoB's is also captured in question 15 below.

Social Security Number

Name

E-Mail Address

Phone Numbers

Medical Notes

Military Status

Date of Birth

Biometric Identifiers

Mailing Address

Medical Records Number

Financial Account Info

Employment Status

STAR: STAR does not collect any data but integrates with CDRAP for its data sources. STAR provides its users the ability to create and share analyses and dashboards through AWS QuickSight. These analyses and dashboards are stored and maintained by STAR. Only the organization has access to the files, so STAR does not have access to what data is being stored to verify that PII/PHI is present, but the files can contain PII/PHI.

STAR contains PHI and PII in whatever form a line of business may contribute and/or produce, including resident, patient assessment, clinical, and provider data. The Personally Identifiable Information (PII) and Protected Health Information (PHI) is used to assist LOBs in their efforts to analyze, explore, report, and create dashboards so issues and trends may be identified to improve quality of care.

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

CDRAP: CDRAP is a cloud-based centralized data repository and internet-facing multi-tool analytic solution that provides timely access to CCSQ quality data and commonly used datasets such as Claims (Part A, Part B, Part D), Complete Statistical Analytic Table (CSAT), beneficiary, provider data used by the Quality Improvement Organizations (QIO) program. So, the CDR contains copies of the original data for all types of PII/PHI that exist in consuming CCSQ Lines of Business and the PII/PHI is regularly used in analysis of quality data to improve patient outcomes. CDRAP does not collect new data; it uses copies of existing datasets from existing QualityNet systems. The data is kept within CDR for as long as needed. Since the data is not the system of record, the data can be dropped if it is no longer needed.

STAR: The STAR system is comprised of non-prod and production environments (Dev, Test, and Production) which each reside in their own dedicated Virtual Private Cloud (VPCs) within the QNet AWS Cloud. Each environment is comprised of shared resources (across all environments) that reside in the Infrastructure Services VPC’s in QNet AWS cloud and is broken into presentation, application, and data zones/subnets.

STAR does not collect any data but integrates with CDRAP for its data sources. STAR provides its users the ability to create and share analyses and dashboards through AWS QuickSight. These analyses and dashboards are stored and maintained by STAR.

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
Biometric Identifiers
E-Mail Address
Mailing Address

Phone Numbers
Medical Records Number
Medical Notes
Financial Accounts Info
Military Status
Employment Status
A copy of the original data(including PII/PHI) that exist in consuming LoBs (Line of Businesses).

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

Patients
CDRAP/STAR: Patients, Physicians, Physician Groups, Dialysis Facilities, Hospitals, Nursing Facilities, and Outpatient Providers.

How many individuals' PII is in the system?

1,000,000 or more

For what primary purpose is the PII used?

CDRAP: The primary purpose is to analyze quality data to improve patient outcomes.

STAR: PII is not used directly by STAR and is collected only when included as part of uploaded files from providers and/or data sources. Users/organizations can upload files through SPICE (Super-fast, Parallel, In-memory Calculation Engine). Only the organization has access to the files in SPICE, so STAR does not have access to what data is being stored, which could include PHI and PII. Users can create analyses through datasets through connected databases which contain PHI/PII.

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

CDRAP: There are no secondary uses for PII data.

STAR: STAR does not have direct secondary uses for PII. The respective organizations the data is mapped to may use PII for secondary uses to support their goals, but this is dependent on each respective organization and not with the input of STAR.

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

CDRAP: ESRD Quality Reporting System, End-Stage Renal Disease (ESRD) Program Management and Medical Information (PMMIS): 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).

Hospital Quality Reporting, Internet-Based Quality Improvement Evaluation System, Quality Management and Review Systems, Standard Data Processing System Data Warehouse, Standard Data Processing System Online, The Case Review Information System (CRIS): Covered by the Code of Federal Regulations (CFR), Title 42 - Public Health, Chapter IV - Centers for Medicare & Medicaid Services DHHS, Subchapter F - Quality Improvement Organizations, PART 480 - Acquisition, Protection, and Disclosure of Quality Improvement Organization Information under the authority of Title 42 U.S.C. sections 1302 and 1395hh. [QIO Regulations 42 CFR PART 480]

Quality Payment Program (QPP): Provisions of the Social Security Act codified at 42 U.S.C. §§¿1320c-3, 13951, 1395w-4, 1395w-21, and 1395y.

STAR: Medicare Improvements for Patients and Providers Act (MIPPA), 1974, Section 153c,

Medicare, Medicaid and SCHIP Extension Act (MMSEA), 2007, Medicare Improvements for Patients and Providers Act (MIPPA), 2008, Health Insurance Portability and Accountability Act (HIPAA), Privacy Rule, Tax Relief and Health Care Act (TRHCA), Affordable Care Act (ACA), 45 CFR 155.210 (e), and 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

Other

Government Sources

Within the OPDIV

Other HHS OPDIV

Non-Government Sources

Media/Internet

Identify the OMB information collection approval number and expiration date

CDRAP/STAR: No OMB information collection approval is needed. PII is not collected directly from the individual about whom the information contains.

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.

CDRAP/STAR: Data Use Agreements (DUAs) are vetted through CMS' Enterprise Privacy Policy Engine (EPPE), which is the CMS system used to track disclosures of data containing PHI or PII. EPPE is required for use by CMS Contracting Officer Representatives (CORs), CMS contractors, and researchers requesting Limited Data Sets (LDSs) to manage their DUAs.

The DUAs for all organizations with whom information is shared or disclosed is maintained by QualityNet Contract Services, via a DUA Tracking Confluence page. This page is updated frequently to reflect the current status of said agreements.

Describe the procedures for accounting for disclosures.

CDRAP: The date, nature and purpose of data sharing and disclosures is described in detail within the DUAs that are maintained by QualityNet Contract Services, via the DUA Tracking confluence page.

STAR: Not Applicable

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

CDRAP: CDRAP is not a source system that collects information directly from any individuals that have PII within the system. Due to this, CDRAP has no required process to notify individuals that their personal information will be collected and stored within the system.

Individual notification for the collection or use of PII is handled by other CMS FISMA systems that are covered under their own existing PIAs. These systems include the Integrated Data Repository (IDR), the ESRD Quality Reporting System (EQRS), Hospital Quality Reporting (HQR), Quality

Payment Program (QPP) with integration of additional datasets also planned for the future.

STAR: STAR does not collect personal information from individuals.

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.

CDRAP/STAR: CDRAP is not a source system that collects information directly from any individuals that have PII within the system. Due to this, there is no required process for handling individual opt-out for the collection or use of PII.

Individual opt-out of the collection or use of PII is handled by other CMS FISMA systems that are covered under their own existing PIAs.

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

CDRAP: CDRAP is not a source system that collects information directly from any individuals that have PII within the system. Due to this, CDRAP has no required process for handling individual opt-out for the collection or use of PII.

Individual opt-out of the collection or use of PII is handled by other CMS FISMA systems that are covered under their own existing PIAs.

STAR: LOBs for this would constitute all systems with a Quicksight entitlement in HCQIS Access, Roles, and Profile Management (HARP). This is listed on the CCSQ QuickSight Organization & Access Catalog.

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.

CDRAP/STAR: Concerns around an individual's PII are fielded by the QualityNet Help Desk.

866-288-8912

qnetsupport@QNet.org

Note that because STAR uses CDRAP as the data source, most changes to data should be made there or the LOB.

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

CDRAP: Data within CDRAP is static once it is loaded into the system and used for analysis purposes only. Data is routinely refreshed from its various sources and goes through integrity checks prior to loading into the system to ensure the data is in the proper format and has not been tampered with.

STAR: STAR periodically reviews resources that are made available to all authenticated QuickSight users. In addition, STAR monitors usage of resources so that any unused resources can be reviewed by the owner organization before being purged.

STAR does not review relevancy but relies on the PII owner organization to deter

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.

CDRAP: CDRAP applies the principle of least privilege as well as role-based method of granting rights. All users are assigned a role and each role's rights are restricted to only data and server resources needed to perform their job. All Production access to data requires a CMS approved Data Use Agreement, as well as CMS approval..

STAR: STAR administrators are able to access system resources through the HCQIS network. Administrative permissions include the ability to access 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.

CDRAP: CDRAP applies the principle of least privilege as well as role-based method of granting rights. All users are assigned a role, and each role's rights are restricted to only data and server resources needed to perform their job.

STAR: STAR is integrated with HARP and divides each shared structure into organizations and roles. A Security Official is designated for each organization to approve access to a particular role within an org. This enforces "need-to-know" and "least privilege."

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.

CDRAP/STAR: 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 Security Training (RBST), DoD Cyber Awareness Challenge (CAC), Identifying and Safeguarding Personally Identifiable Information (PII), Records Management Training (RMT), Information Systems Security and Privacy Awareness Training (ISSPA) and review and sign off on the Rules of Behavior (ROB) 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/onboarding.

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

CDRAP/STAR: 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 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.

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.

CDRAP: The CMS Acceptable Risk Safeguards (ARS), QualityNet Security and Privacy Policy Framework and QualityNet Contractor Furnished Equipment (CFE) Use and Data Management Guide provide the guidance on how to protect media through proper access controls, media marking, media transportation, proper media sanitization techniques, and controls for sanitization and disposal decisions considering the security categorization of the associated system's confidentiality. Data is stored and destroyed following the CMS Records schedule which follows National Archives and Records Administration (NARA) General Record Schedules (GRS). Per Disposition Authority: N1-440-09-3, Temporary. Cutoff annually. Delete/destroy when 10 years old, or when no longer needed for Agency business, whichever is later.

CDRAP does not review relevancy but relies on the PII owner organization to determine this.

STAR: STAR periodically reviews resources that are made available to all authenticated QuickSight users. In addition, STAR monitors usage of resources so that any unused resources can be reviewed by the owner organization before being purged.

STAR does not review relevancy but relies on the PII owner organization to determine this.

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

CDRAP/STAR: 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, off site 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, fire walls, Intrusion Detection and Prevention systems (IDS/IPS), hardware configured with 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.

All infrastructure supporting PII storage and use is in the CMS network which requires verified, authenticated

Redshift -
The computation engine for QuickSight, the cluster requires encryption at rest and in transit, contains full log auditing, has restrictive VPC Security Groups, and management of the cluster is restricted specifically to administrators.

CDRAP Integration -
Within the Redshift cluster, schemas will be mounted using role chaining: the IAM role assumed by the Redshift cluster assumes the role maintained by the CDRAP team.

S3 Storage -
All buckets have block public access rules enabled at the org and bucket level. Access Control Lists and policies are attached to constrain use to QuickSight and the AWS administrative account.

QuickSight IAM -

For users to be able to access their organizational data, STAR integrates with HARP SavyInt to map SavyInt roles to QuickSight groups. Security Officials approve or reject role requests to enforce least privilege.

Identify the publicly-available URL:

CDRAP:

ccsqdatacatalog.cms.gov
preprod.ccsqdatacatalog.cms.gov
impl.ccsqdatacatalog.cms.gov
dev.ccsqdatacatalog.cms.gov
ccsqdataanalytics.cms.gov
dev.ccsqdataanalytics.cms.gov
qnetanalytics-databricks.cms.gov
dev.qnetanalytics-databricks.cms.gov
impl.qnetanalytics-databricks.cms.gov
preprod.qnetanalytics-databricks.cms.gov
preprod.ccsqdataanalytics.cms.gov
impl.ccsqdataanalytics.cms.gov
da-cdr-prod.cloud.databricks.com
da-cdr-dev.cloud.databricks.com
da-cdr-impl.cloud.databricks.com
da-cdr-preprod.cloud.databricks.com

STAR: Not available for the general public
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