# US Department of Health and Human Services

## Privacy Impact Assessment

### Date Signed:

02/16/2017

### OPDIV:

CMS

### Name:

Data Support and Feedback Reporting Data Hub

**PIA Unique Identifier:**

P-3045556-016798

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

Minor Application (child)

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

Implementation

**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)?**

No

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

**Describe the purpose of the system.**

The Data Support and Feedback Reporting Data Hub was developed to support the Transforming Clinical Practice Initiative (TCPI) model. The model will test whether a three-pronged approach to national technical assistance will enable large scale transformation of thousands of clinician practices to deliver better care and result in better health outcomes at lower costs for Medicare, Medicaid, and Children’s Health Insurance Program (CHIP) enrollees. This initiative seeks to prepare practices for upcoming payment reforms that emphasize quality of care over quantity of care.

The TCPI initiative is designed to support more than 140,000 clinician practices over the next four years in sharing, adapting and further developing their comprehensive quality improvement strategies. The initiative is one part of a strategy advanced by the Affordable Care Act to strengthen the quality of patient care and spend health care dollars more wisely. It aligns with the criteria for innovative models set forth in the Affordable Care Act:

Promoting broad payment and practice reform in primary care and specialty care,

Promoting care coordination between providers of services and suppliers,

Establishing community-based health teams to support chronic care management, and

Promoting improved quality and reduced cost by developing a collaborative of institutions that support practice transformation.

The TCPI Data Hub supports this effort through data ingest, analysis, dashboards, and reports.

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

Practice Transformation Networks (PTNs) and Support & Alignment Networks (SANs) will submit reports that contain aggregate information about the practices they reside over as well as clinician recruitment data. For release 1, Personally Identifiable Information (PII) data will be limited to the submitted TCPI / SAN recruitment reports which will contain Taxpayer Identification Numbers (TINs).

The following provider information will be collected, stored, and maintained by the TCPI Data Support and Feedback Reporting (DSFR) application:

Provider Enrollment Information: First Name, Last Name, Email Address, National Provider Identifier (NPI), Group or Organization Name, Group or Organization Address (Street, City, State, Zip), Group or Organization Point of Contact (POC) Name, POC Email, POC Phone number, Group or Organization Employee Count, Individual Group or Organization Taxpayer Identification Number (TIN) Number, Support Alignment Network description

Clinical Measures Information: Names, Descriptions, Standards, Action, Network Name, Percentages, Scores

Participant Information: Patient Count, Patient Race, Patient Below Deprivation Line Percent, Patient Count Total Number, Patient Dual Eligible Percent, Patient Medicaid Percent, Patient Medicare Percent, Patient Primary Language English Percent

User credentials for access to the TCPI DSFR application are handled by the CMS Enterprise Identity Management (EIDM) which is separately accredited and has its own PIA. Users will navigate to the CMS Innovation Center (IC) Landing Page, select the DSFR application, and then be prompted for EIDM user credentials- user ID and password. If the user does not have an existing EIDM account, they will be provided the online form to register.

User credentials for direct contractor backend access to DSFR are managed through Amazon Web Services (AWS) by the Infrastructure Contractor for the CMS AWS instance, General Dynamics. Users are required to first register with the CMS Enterprise User Administration (EUA) which has its own PIA and request the proper job codes (requiring CMS Access Administrators (CAA) and Contracting Officer Representative (COR) approval) to allow them. Jira and EUA are used to request and get approval for specific roles, group member ship and access. Users must request specific job codes for specific access through EUA. EUA Job codes define the access to the applications and roles needed within the application. Least privilege access is enforced using this method. There are no user credentials stored within the DSFR application boundary, however, user ID and password are collected for access.

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

The system will receive Personally Identifiable Information (PII) from the PTNs, SANs, and Quality Improvement Organizations (QIOs) in order to perform analyses and reporting for a multitude of performance metrics that support the CMS Transforming Clinical Practice Initiative (i.e., compliance, progress, benchmarks, comparisons, and performance trends). The data transformation process includes required quality validation, attribution, unification, aggregation and correlation that will support desired reporting and visualization needs. Some de-identified TCPI metadata will be published on a public visualization platform (Socrata). No PII or other sensitive data are shared via the public visualization platform. All PII data will be accessed by authorized CMS users and CMS business partners via the restricted Federal Information Security Modernization Act (FISMA) Moderate intranet site.

User credentials for access to the TCPI DSFR application are handled by the CMS Enterprise Identity Management (EIDM) which is separately accredited and has its own PIA and SORN. Users will navigate to the CMS Innovation Center (IC) Landing Page, select the DSFR application, and then be prompted for EIDM user credentials. If the user does not have an existing EIDM account, they will be provided the online form to register.

User credentials for direct contractor backend access to DSFR are managed through Amazon Web Services (AWS) by the Infrastructure Contractor for the CMS AWS instance, General Dynamics. Users are required to first register with the CMS Enterprise User Administration (EUA) and request the proper job codes (requiring CMS Access Administrators (CAA) and Contracting Officer Representative (COR) approval) to allow them. Jira and EUA are used to request and get approval for specific roles, group member ship and access. Users must request specific job codes for specific access through EUA. EUA Job codes define the access to the applications and roles needed within the application. Least privilege access is enforced using this method.

There are no user credentials stored within the DSFR application boundary.

**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

Medical Records Number

Medical Notes

Taxpayer ID

Other: National Provider Identifier (NPI), Group or Organization Name, Group or Organization

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

Employees

Business Partner/Contacts (Federal/state/local agencies)

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

500-4,999

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

The DSFR Team uses PII to analyze model progress towards the seven program goals and provide insights regarding the model to CMS and other stakeholders.

The user account information is used in order to authenticate and provide access to the system users for system support and also to perform their work.

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

N/A

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

§ 1110 of the Social Security Act (the Act), which authorizes research and demonstration projects under Social Security Act programs;

§ 1115 of the Act, which authorizes Medicaid demonstrations; and § 402 of the Social Security Amendments of 1967 (42 U.S.C. 1395b– 1), which authorizes waivers of Medicaid and Medicare provisions under certain demonstrations.

**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.**

Development and Information (ORDI), System NO. 09-70-0591

Master Demonstration Evaluation, and Research Development and Information (DERS), for the

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

Online

**Government Sources**

State/Local/Tribal

Other

**Non-Governmental Sources**

Private Sector

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

PII data is collected secondary to the care providers who will provide to DSFR for approved research purposes, under the statutory authorities cited earlier in this PIA. User credential information is not subject to OMB Collection Approval.

**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.**

PTNs, SANs, and QIOs are notified by the DSFR application when they access the tool and prepare to voluntarily submit their provider information. Users are provided with a Terms of Service / System Use Notification as well as a Privacy Notice.

**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.**

TCPI participants (PTNs, SANs, and QIOs) consent to use of their PII as a condition of participating in the TCPI program to help measure performance and improve CMS programs and outcomes. If intended participants do not provide their PII, they will not be able to participate, however participation is not a federal requirement and there is no legal impact.

System users cannot opt-out of use of their user credentials since it is required to perform their job duties.

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

Any major change to the system or change in intended use of PII is communicated to providers via the DSFR application, TCPI stakeholder email distribution, and TCPI stakeholder community memos. A new PIA and System of Record Notice (SORN) may also be issued depending on the scope of the change.

**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 with concerns about PII collection and disclosure are referred to the local QIO Security Point of Contact (SPOC). If the QIO is not able to assist the individual directly, they will raise the issue to the Quality Net Enterprise Service Desk by issuing a ticket.

Users of the system can contact the EIDM Help desk or the EUA help desk in order to resolve an issue with their account information.

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

DSFR adheres to the CMS Acceptable Risk Safeguard (ARS) 2.0 controls, a subset of which focus on PII and ensuring its confidentiality, integrity, and availability. No integrity checks are performed since the PII data in the system is provided as a secondary use for approved performance evaluation purposes. Inaccurate PII data would only have limited impacts on the system or how it is used by CMS and PTNs/SANs/QIOs.

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

**Administrators:**

Administrators have access to the system to ensure it is running properly. Generally, PII access is not necessary to resolve issues, but in some cases it is necessary. Administrators sign non-disclosure agreements and take annual CMS-required security and privacy training as a requirement of their role.

**Developers:**

Developers have access to the PII for development and testing purposes for system enhancements, fixes and provider assistance (help desk). Developers sign non-disclosure agreements and take annual CMS-required security and privacy training as a requirement of their role.

**Contractors:**

Direct contractors are comprised of administrators and help desk personnel. Direct contractors may have access to PII for purposes of troubleshooting user and system issues. Direct contractors sign non-disclosure agreements and take annual CMS-required security and privacy training as a requirement of their role.

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

System support direct contractors are approved by the business owner and are each assigned to approved roles that will ensure users only have access to the minimum amount of information necessary to perform their assigned duties.

**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 relies on role based access controls. Users are granted permissions based on pre-defined roles associated with their approved job codes.

**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 annual 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).**

System users 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.**

In accordance with SORN 09-70-0591, CMS will retain identifiable information maintained in the DERS system of records for a period of 5 years after the end of the research, demonstration, or evaluation project. System access information is under DAA-GRS-2013-0006-0003- Destroy 1 year (s) after user account is terminated or password is altered or when no longer needed for investigative or security purposes, whichever is appropriate.

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

CMS Virtual Data Center/Amazon Web Services (AWS): Secure File Transfer will receive TCPI / SAN data and Booz Allen staff will access data via AWS virtual machines with encrypted storage. PII will be stored in Amazon using encryption. Least privilege role based permissions will be used to ensure appropriate access to all systems and data. Hosted 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: Assessment and Authorization (A&A), annual security assessments, monthly management of outstanding corrective action plans, ongoing risk assessments, and automated continuous monitoring.