US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

11/13/2017

OPDIV:

CMS

Name:

Services Tracking Analysis and Reporting System on the IDR

PIA Unique Identifier:

P-1673091-300261

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.

Agency

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.

CMS utilizes the Services Tracking Analysis and Reporting System (STARS) Informant anti-fraud data analysis product to perform analysis for the detection and investigation of potential fraud, waste, and abuse in the Medicare Fee-For-Service (FFS) program on the Integrated Data Repository (IDR).

The STARSInformant application allows users to query database views in the IDR to locate potential fraud, waste, and abuse in the Medicare Program.

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

The STARS IDR consists of Medicare data from the National Claims History (NCH) and the CMS Shared Systems. This data consists of claims data as well as ancillary data for beneficiaries, providers, health plans, drug data and clinical data.

The claims data contains Personally Identifiable Information (PII), including Name, Date of Birth (DOB), Social Security Number (SSN), Health Insurance Claim Number (HICN), mailing address, telephone numbers, financial records, medical notes, medical record number, patient ID, certificates, device identifiers and employment status.

The STARS application also maintains user's (CMS direct contract support) first and last name, email address, phone number user ID and password.

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

The STARSInformant application allows users to log in via CMS Enterprise Identity Management (EIDM). EIDM collects and maintains user credentials on behalf of the STARS application. After users are authenticated to the system, they are able to query database views in the IDR to locate potential fraud, waste, and abuse in the Medicare Program. The data queried from the IDR contains PII, including Name, DOB, SSN, HICN, mailing address, telephone numbers, financial records, and employment status. STARS does not collect PII but maintains it once provided by NCS and IDR. This data is used in support of fraud, waste, and abuse investigations and litigations within the Medicare Program.

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

Financial Accounts Info

Certificates

Device Identifiers

Employment Status

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

Employees

Patients

How many individuals' PII is in the system?

100,000-999,999

For what primary purpose is the PII used?

Law enforcement personnel and fraud, waste, and abuse detection and prevention direct contractors use this data in support of Fraud, Waste, and Abuse investigations and litigations within the Medicare Program.

System user's credentials are used for granting access to the system for normal operations and maintenance.

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

Secondary usage of PII in STARSInformant is used for testing and training.

Describe the function of the SSN.

The SSN identifies individual's data within the application.

Cite the legal authority to use the SSN.

Authority is given under Sections 1874 (a) and 1875 of the Social Security Act and Title 42 United States Code (U.S.C.) section 1395kk(a) and 139511.

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

Authority is given under Medicare Prescription Drug Improvement and Modernization Act of 2003 (MMA) (Pub. L. 108-173)

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.

09-70-0558 - National Claims History

Identify the sources of PII in the system.

Online

Government Sources

Within OpDiv

Identify the OMB information collection approval number and expiration date

Not applicable for user credentials.

Is the PII shared with other organizations?

Yes

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

State or Local Agencies

Law enforcement is afforded access to the STARSInformant application after proper vetting occurs to investigate potential fraud, waste, and abuse in the Medicare Fee-For-Service (FFS) program.

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

Every user of STARS acknowledges his/her Data Use Agreement prior to receiving access to the system. The STARS application also executes a Memorandum of Understanding (MOU) between STARS and IDR.

Describe the procedures for accounting for disclosures.

All users of STARSInformant are required to sign and read the Data Use Agreement (DUA) for all data requests including PII. The DUA describes the purpose of the disclosure, the data disclosed and with whom it is disclosed to. Data Use Agreements are maintained by CMS and stored in the CMS Federal Information Security Management Act Controls Tracking System (CFACTS). It is also available in hard copy files. STARS logs all database views queried by each individual agency.

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 Services Tracking Analysis and Reporting System(STARS) does not directly collect the information about individuals. The systems that collect the information directly from the individuals provide that notice.

For the CMS contractor's user credentials, written notice is provided when they apply for a job.

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.

STARS does not directly collect the information about individuals so there is not a method for individuals to opt out of collection of their information.

The CMS contractors cannot opt out of providing PII because the collection of the data is necessary for employment.

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

The process for obtaining consent for any individual's information submission would occur at the provider or authorized billing agent which occurs outside of this application.

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.

STARS does not collect individual identifiable information, thus the process of resolving individual concerns would be the responsibility of the provider or authorized billing agent which occurs outside of this application.

To resolve complaints about user credential information, CMS Contractors call the CMS IT help desk and the complaint will be resolved accordingly.

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

There is no data collection of Personally Identifiable Information within the STARS application; therefore a review of the data integrity is not performed. Data integrity is performed upstream from the STARS application at the provider location or responsible billing agent.

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

Users:

To detect fraud, abuse, and waste in the Medicare FFS program.

Administrators:

To grant access to the system and perform system administration.

Contractors:

To maintain systems and support end users.

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

STARSInformant access is authorized and approved by the system business owner. All users that require access are assigned a job code that restricts that access to 'least privilege' and 'need to know'.

Contractors, end users and administrators must recertify their system access annually, which aligns with CMS security policy requirements.

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 is role based and designed based on least privilege, explicitly denied unless otherwise granted. The user roles are reviewed a minimum of semi-annually to ensure the access is still necessary.

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.

CMS Security Awareness and Privacy training is provided to each user on an annual basis. All system maintainers, managers, and contractors must acknowledge successful completion of the training. The training covers privacy and security controls for access to any and all CMS information systems. Included in the training is education about how to properly handle sensitive data. If the

training is not completed, the user's CMS user account is revoked.

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

STARS IDR provides user training to new users and periodic updates to all users.

Also, prior to exporting data users receive a HIPAA Confirmation Request stating "This data may contain confidential information subject to the HIPAA Standards for Privacy of Individually Identifiable Health Information. Would you like to proceed?"

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.

Data retention and destruction falls under the responsibility of the IDR system maintainer. All data is maintained in the IDR and STARS does not collect PII directly from individuals or maintain a separate database.

NARA Requirements for IDR:

Destroy no sooner than 7 year(s) after cutoff but
longer retention is authorized
(DAA-0440-2015-0012-0001)

Master Files; Disposition: Delete/Destroy when 10 years old or when no longer needed for Agency business, whichever is later (DAA-0440-2012-0004-0001).

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

The CMS administrative, technical, and physical security requirements are followed, which provide a security in depth approach to maintaining the confidentiality, integrity, availability, and privacy of sensitive data. The system is assessed annually by an independent audit firm to assure compliance with all CMS Security requirements, whether administrative, technical, or physical.

Administrative: Only registered users can access the data after being approved via a rigorous vetting process.

Technical: The Services Tracking Analysis and Reporting System operates behind secure firewalls which may track any anomalies and report to a central security operations center (SOC) for necessary action. System monitoring is performed in real time to ensure any and all system vulnerabilities are patched within the required timeframe.

Physical: The data is located inside a secure datacenter only accessible to approved datacenter personnel. Access to the facility is monitored by security guards and Closed Circuit Television (CCTV). Visitors must present a valid government ID and be escorted through the facility.