US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

09/23/2016

OPDIV:

CMS

Name:

Single Testing Contractor

PIA Unique Identifier:

P-7736863-079917

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?

Existing

Does the system have Security Authorization (SA)?

Yes

Date of Security Authorization:

7/11/2016

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.

No changes were made since last PIA review.

Describe the purpose of the system.

The Single Testing Contractor (STC) system is the CMS testing system for the Fee for Service (FFS) Shared Systems. The STC is responsible for testing the FFS claims processing systems in a fully-integrated way, which includes data exchanges with all key connected systems: Fiscal Intermediary Standard System (FISS), Multi Carrier System (MCS), ViPS Medicare System (VMS), Common Working File (CWF), Healthcare Integrated General Ledger Accounting System (HIGLAS), Coordination of Benefits Contractor (COBC), and Provider Enrollment Chain and Ownership System (PECOS). The connected systems, which are covered by separate PIAs, process billions of dollars in claims, which directly impacts the CMS Financial Statement.

The STC'c Integration Testing Program supports high quality system changes by finding and resolving defects prior to implementation of the changes, and improves standardization across the FFS shared systems through a single control point and source of accountability. This program allows CMS to monitor and control system testing, costs, standardization, communication and flexibility across systems. This system utilizes claim data to assure processes are functioning correctly.

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

The STC testing systems use claim data, which contains PII and PHI (protected health information), obtained from other contractors as well as developing test data to test the systems functions.

The STC uses sample Medicare claims Part A and Part B data, which contains PII/PHI, in testing the Fiscal Intermediary (FI) claims processing, the Fiscal Intermediary Standard System (FISS), the Multi Carrier System (MCS), the Durable Medical Equipment, Prosthetics, Orthotics, and Supplies (DMEPOS) carrier claims processing, Medicare Administrative Contractors (MAC) claims processing, the ViPS Medicare System (VMS), the Common Working File (CWF), and the Healthcare Integrated General Ledger Accounting System (HIGLAS).

The information used includes name, social security number, date of birth, health insurance claim number, mailing address, phone numbers, medical record numbers, medical notes, financial account information, certificates, device identifiers, email address, military status and/or records, health insurer name/plan, health insurer group number, patient marriage and employment status; claims forms for the purpose of processing and paying claims.

In order for CMS employees and direct contractors to be granted access to STC the user must provide their User ID and Password. The Users IDs and Passwords are managed by the Enterprise User Administrator (EUA) system.

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

The purpose of the Single Testing Contractor (STC) contract is for CMS to obtain the ongoing test site(s) and technical support services to fully test the Fiscal Intermediary (FI) claims processing, the Fiscal Intermediary Standard System (FISS), the Multi Carrier System (MCS), the Durable Medical Equipment, Prosthetics, Orthotics, and Supplies (DMEPOS) carrier claims processing, DMAC claims processing, the ViPS Medicare System (VMS), the Common Working File (CWF), and the Healthcare Integrated General Ledger Accounting System (HIGLAS).

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

Military Status

Employment Status

Other - Health Insurance Claim Number (HICN), medical records, health insurer name/plan, health

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

Employees

Public Citizens

Patients

How many individuals' PII is in the system?

1,000,000 or more

For what primary purpose is the PII used?

The Single Testing Contractor (STC) uses PII to fully test application system changes to the various systems of CMS to ensure accurate calculations in benefits and payments.

Users Credentials are used to grant system users access in order to support the operations and maintenance of the system.

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

NA

Describe the function of the SSN.

NA

Cite the legal authority to use the SSN.

Authority for the maintenance of this system of records is given under the authority of sections 1816, and 1874 of Title XVIII of the Social Security Act (42 U.S.C.1395h, and 1395kk).

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

Sections 1842, 1862 (b) and 1874 of Title XVIII of the Social Security Act (The Act) (42 United States Code (U.S.C.) 1395u, 1395y (b), and 1395kk)

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.

This system is covered under the SORN's of the systems it supports. Those systems are:

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Online

Government Sources

Within OpDiv

Non-Governmental Sources

Public

Private Sector

Identify the OMB information collection approval number and expiration date

No OMB collection approval is needed because PII is not collected directly from individuals with whom the information pertains and an OMB approval is not applicable to user credentials.

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.

There is no process in place to notify individuals that their personal information will be collected because the data used by the STC system has already been collected by other systems that have processes in place to notify individuals that their data will be collected. These systems, FISS, MCS and CWF, are all covered under the own PIAs. All data used by the STC is treated as test data. No actual claim data updates are made. For the CMS direct contractors and CMS employees, 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.

Since STC does not collect PII/PHI directly from individuals whose PII/PHI is used by the testing systems, there is no need for implementing a process to notify and obtain consent.. The CMS direct contractors and CMS employees 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.

All data used by STC is test data. Therefore we do not notify the individuals about the use or changes to their PII. No changes are ever made by the STC to the application system(s) of record. The CMS direct contractors and CMS employees would be notified under their employment.

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.

No process exists because all data used by STC is test data. We do not update live data for the systems we test. Therefore no individual's data is changed in the system(s) of record.

The CMS direct contractors and CMS employees would report to the contractor IT service desk or security officer as soon as an incident comes to the attention of an information system user. All confirmed security incidents and events shall be reported to the CMS IT Service Desk in accordance with the procedures set forth in the CMS Information Security Incident Handling and Breach Analysis/Notification Procedure.

When reporting confirmed security incidents, CMS direct contractors and CMS employees shall report the date and time when events occurred or were first discovered; names of systems, programs, or networks effected by the incident; and impact analysis. Release of information during incident handling shall be on an as-needed and need-to-know basis.

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

No process for claim data needed since the data is used as test data only. The CMS contractors and CMS employees have annual PII recertification reviews.

In order to maintain the integrity, availability, accuracy, and relevancy of the PII stored within the database, the System Administrator, semi- annually, performs a crosswalk between the EUA listing of individuals with the appropriate job code and STC's listing of active users. Any anomalies (i.e. name change, or mismatch) is addressed and resolved by contacting the user, and modifying their user data, or by removing their access to STC, if no longer required under their current job description.

Under this process, outdated, unnecessary, irrelevant, and inaccurate PII is identified and deleted from STC. The PII is available as needed, and is sufficient (minimum required) for the purposes needed. The PII fields are locked and cannot be changed; The process to ensure that individuals who provide or modify PII cannot repudiate that action is done within the source (EUA) system. The process to ensure PII is available when needed is by having nightly updates run between the EUA systems and STC; the process to ensure that PII is sufficiently accurate for the purposes needed is ensured when the nightly updates are sync. Users, can at any time, request that their PII (access) be deleted, by contacting their CMS Access Administrator (CAA), who in turn, would take the corresponding action via EUA.

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

Administrators:

Administer testing

Developers:

Developer/Programmers are granted temporary access in order to fix and ensure that errors are fixed

Contractors:

Conduct Testing

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

STC uses role-based access limitations and least privilege controls to restrict PII availability. There is a CMS Access Administrator (CAA) and System Administrator who oversees the job role approval.

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.

Administrators and direct contractors have ROLE based access which limits their access to PII data.

Users must have a STC job code in their EUA user profile before they are granted access to STC.

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.

System users must complete annual CMS Computer Based Training Privacy and Security training with a score of 100% before being granted access to the system. We do not collect or maintain PII for any purpose other than testing.

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

Administrators are trained via on the job training in the responsibilities and duties of their role in STC.

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.

Per National Archives and Records Administration (NARA): PII records are retained temporarily. Cutoff at the end of the fiscal year (FY). Delete/destroy 6 years and 3 months after cutoff, or when no longer needed for Agency business, whichever is later.

(Disposition Authority: N1-440-09- 14)

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

Access to the systems is given based on need to know and job responsibilities to process Medicare claims. Medicare Claims Processing Standard Systems maintainers use security software and methods to provide “least privilege access.” They will utilize software which as a part of the security systems that provides access control and auditing functionality, the ability to grant or deny access to data based upon need to know.

Sometimes, in order to fix programmatic problems, programmers are granted temporary access in order to fix and ensure that errors are fixed. The temporary access may be granted for a day or other short periods of time that can be controlled through security software. External audits also verify these controls. Technical controls used include user identification, passwords, firewalls, virtual private networks and intrusion detection systems. Physical controls used include guards, identification badges, key cards, cipher locks and closed circuit televisions.