US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

06/02/2016

OPDIV:

CMS

Name:

Eligibility Support Desktop Change Utility Tool

PIA Unique Identifier:

P-7542519-203964

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?

New

Does the system have Security Authorization (SA)?

Yes

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

Describe the purpose of the system.

The Eligibility Support Desktop Change Utility Tool (ESDCU) is an internal tool for CMS to update consumer information in the Federally Facilitated Marketplaces (FFM) eligibility and enrollment records. The ESDCU allows edits, corrections and updates of consumer data to assist with appeals and eligibility determinations of consumers participating in the FFM. FFM transmits the information to ESDCU for the off-line capturing/editing of information and submission back into FFM for effectuation.

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

The ESDCU processes files, which contain the social security number (SSN), name, driver’s license number, mother’s maiden name, email address, phone number, military status, taxpayer identification, date of birth, mailing address, legal documents, employment status, wage data and immigration documents about consumers enrolled in or applying for healthcare coverage through FFM.

ESDCU users are CMS employees and direct contractors serving the FFM help desk to help consumers. Access to ESDCU is managed in two ways. The ESDCU case workers access the system through the CMS Enterprise Identity Management (EIDM) website and select the ESDCU tool within that environment. They do not enter user credentials directly into ESDCU for accessibility. Login credentials are entered into the EIDM system and are managed by that system. The EIDM has its own Privacy Impact Assessment (PIA) about the information contained within it.

The second group of users is system administrators. Those users access ESDCU through a separate tool called CyberArk.
CyberArk is managed by the Marketplace Exchange Operations Center (XOC). CyberArk access requires XOC management approval for each access and assigns temporary access (username/password) to the account. The XOC has its own PIA for the information that is handled by that system.

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

The ESDCU is a CMS internal tool for making updates to the FFM eligibility and enrollment records in support of case work relating to eligibility appeals, support and information corrections. ESDCU was developed to allow for off-line capturing/editing of information and submission back into FFM for effectuation. The information transmitted to ESDCU is about consumers enrolled in or attempting to enroll in the FFM. This includes the consumer’s name, address, phone number and other information needed to enroll in the FFM. The information in ESDCU is maintained temporarily and the corrected information is transmitted back to the FFM system.

ESDCU users are CMS employees and direct contractors serving the FFM help desk to help consumers. Access to ESDCU is managed in two ways. The ESDCU case workers access the system through the CMS Enterprise Identity Management (EIDM) website and select the ESDCU tool within that environment. They do not enter user credentials directly into ESDCU for accessibility. Login credentials are entered into the EIDM system and are managed by that system. The EIDM has its own PIA about the information contained within it.

The second group of users is system administrators. Those users access ESDCU through a separate tool called CyberArk.
CyberArk is managed by the Marketplace Exchange Operations Center (XOC). CyberArk access requires XOC management approval for each access and assigns temporary access (username/password) to the account. The XOC has its own PIA for the information that is handled by that system

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

Driver's License Number

Mother's Maiden Name

E-Mail Address

Mailing Address

Phone Numbers

Legal Documents

Military Status

Employment Status

Taxpayer ID

Other - Wage data; Immigration Documents.;

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

Public Citizens

How many individuals' PII is in the system?

10,000-49,999

For what primary purpose is the PII used?

PII is used for the purpose of updating/editing/correcting the information on consumers enrolled in or applying for healthcare coverage through FFM. The consumer data
is not collected directly from the general public.

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

Not Applicable.

Describe the function of the SSN.

Per the Affordable Care Act, Section 1411; CMS must collect the SSN for use in determining citizenship and immigration
status. The SSN will also be used for validating or ID proofing an individual's identity prior to enrollment in the FFM. The SSN is not collected directly by ESDCU and is not shared with any other CMS system

Cite the legal authority to use the SSN.

42 U.S.C. Section 18081 Affordable Care Act, Section 1411

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

Legal authorities include the Patient Protection and Affordable Care Act (PPACA; Public Law 111-148), Title 42 U.S.C. 18031, 18041, 18081,18083, and sections 2723, 2761 of the Public Health Service Act (PHS Act).

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.

09-70-0560, Health Insurance Exchanges (HIX) Program, published 2/6/2013, and updated

Identify the sources of PII in the system.

Government Sources

Within OpDiv

Non-Governmental Sources

Private Sector

Identify the OMB information collection approval number and expiration date

Not applicable as no PII is collected directly from individuals (including user credentials for system access).

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 about the collection of personal information because the ESDCU does not directly collect PII, it is transferred from the FFM system. FFM will outline any processes for notification. Also, system users access ESDCU through other CMS systems, EIDM and CyberArk/XOC. Those systems would notify 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.

There is no method for individuals to opt-out of the collection or use of their PII because the ESDCU does not directly collect PII, it is transferred from the FFM system. FFM will outline any processes for notification. Also, system users access ESDCU through other CMS systems, EIDM and CyberArk/XOC. Those systems would notify individuals.

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

The PII within this system is not collected by ESDCU, so there is no process to notify and obtain consent from individuals should any major changes occur to it. PII is transferred from the FFM system. FFM will outline any processes for notification. Also, system users access through other CMS systems, EIDM and CyberArk/XOC. Those systems would notify individuals about any major changes to the collection of personal information.

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.

There is no process in place to resolve an individual's concerns about their PII, because the ESDCU does not directly collect PII, it is transferred from the FFM system. However an individual can contact the FFM Health Insurance Marketplace call center at 1-800-318- 2596, with concerns that their PII may have been inappropriately obtained, used, disclosed or is inaccurate.

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 PII within this system is not collected by ESDCU. The PII is collected from the individual by another CMS system, which is FFM, and that PIA should reflect how this process is addressed.

Centers for Medicare and Medicaid Services (CMS) has a continuous monitoring program based on the National Institutes of Science and Technology (NIST) recommendations to ensure system integrity, availability. The individual enrollment application is designed with logic checks to ensure data accuracy and integrity. Centers for Medicare and Medicaid Services (CMS)/Center for Consumer Information and Insurance Oversight (CCIIO) has established an Enrollment Resolution and Reconciliation program to provide services necessary to resolve errors and reconcile discrepancies in enrollment data between the Health Insurance Exchange, State Based Marketplaces, issuer community, and CMS. Yearly, CCIIO is required to review and update the enrollment process to ensure data collected is relevant to the health insurance enrollment process.

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

Users:

Users have access to PII to perform the function of ESDCU: update consumers' information in connection with eligibility and enrollment in the FFM.

Administrators:

Administrators have access to PII to review user accounts, provide support to the application process and investigate problems that may contain PII.

Contractors:

CMS direct contractors, as users or administrators would have access to PII in conjunction to those roles and job functions.

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

Individuals requesting access must sign an Account request form prior to account creation, it indicates the level of access required. This form is reviewed and approved by the System Information Security Officer (ISSO) prior to account creation. ESDCU uses the principle of least privilege as well as a role based access control to ensure system administrators and users are granted access on a "need-to-know" and "need-to-access" basis.

System administrators review user accounts at least semi-annually. Any anomalies is addressed and resolved by contacting the user, and modifying their user data, or by removing their access if no longer required. Activities of all users including system administrators are logged and reviewed by ESDCU ISSO to identify any unusual activity.

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.

ESDCU uses the principle of least privilege as well as a role based access control to ensure system administrators, and users are granted access on a "need-to-know" and "need-to- access" commensurate with their assigned duties.

An audit log is maintained to record and review all the activities of users, including system administrators, and is reviewed by ESDCU ISSO to identify any abnormal activities.

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 employees and direct contractors who access or operate a CMS system are required to complete the annual CMS Security Awareness training provided as a Computer Based Training (CBT) course. Individuals with privileged access must also complete role- based security training.

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

Not Applicable.

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.

The ESDCU system follows the National Archives and Records Administration (NARA), Disposition Authority Number DAA-0440-2014- 0001, which is for all systems under the HIX SORN. It states that records will be destroyed 10 years after cutoff, which is the end of the calendar year in which the record is closed or no longer actively used, added to or otherwise modified. The DAA will be incorporated into the CMS Records Schedule by the end of 2016.

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

ESDCU is hosted in a Verizon data center, a Tier III data center which provides the physical control protections. The physical controls are security guard presence, identification checks, and video monitoring on the interior and exterior of the building.

The technical controls in place are intrusion detection/prevention systems, encryption of data, firewalls and application vulnerability scans. Additionally, administrative access is ESDCU uses the principle of least privilege as well as a role based access control to ensure system administrators, and users are granted access on a "need-to-know" and "need-to- access" commensurate with their assigned duties.

The administrative controls in place to secure the PII include access control - request and authentication through the CMS EIDM system, periodic review of users and deletion of non- active accounts. Access to ESDCU is based on the principle of least privilege to ensure system administrators and users are granted access on a "need-to-know" and "need-to- access" basis.