US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

04/30/2024

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?

Existing

Does the system have Security Authorization (SA)?

Yes

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.

The major changes to the Eligibility Support Desktop Change Utility Tool (ESDCU) since the last PIA are:

Eligibility and subsidy changes related to the American Rescue Plan and Inflation Reduction Act.

Changes related to decoupling ESDCU from Federally Facilitated Marketplace (FFM).

Neither of these changes pose a privacy risk or add PII to ESDCU.

Describe the purpose of the system.

The Eligibility Support Desktop Change Utility Tool (ESDCU) is an application that provides access to search and display consumer, insurance application and enrollment data, makes limited eligibility redeterminations, and allows users to open special enrollment periods (SEPs).

The core capability is search and display of data housed in Federally Facilitated Exchange (FFE) through Application Programming Interfaces (APIs).

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

The ESDCU collects audit records that show user activity within the system, and information related to users' editing sessions. Audit records are not purged and are persisted indefinitely. User session info is retained until the end of the user's editing session, to a maximum of 24 hours. User session information includes Social Security Number, Driver's License Number, Email address, Date of Birth (DOB), mailing address, Name, Mother's Name, Phone number, Legal documents, Tax information, immigration documents, wage data.

No information from insurance applications, policies, or plans is persisted in ESDCU. No Personal Identifiable Information (PII) is persisted in ESDCU. User IDs are persisted as part of audit records to identify the user who made changes to an insurance application, but no other information about the user is retained.

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 Federally Facilitated Marketplace (FFM) eligibility and enrollment records in support of case work relating to eligibility appeals, support, and information corrections. The ESDCU was developed to allow for off-line capturing/editing of information and submission back into the Federally Facilitated Exchange (FFE) for effectuation. The information transmitted to ESDCU is about consumers enrolled in or attempting to enroll in the FFE. The ESDCU regularly uses PII to validate a consumer's eligibility to apply for and receive healthcare via the FFE and includes the consumer's name, address, phone number and other information. Audit information is collected because it is a business requirement. User session information is collected to keep track of each user's changes made during the session, and to enable the changes to be saved back to the FFM.

The ESDCU uses the Marketplace Consumer Record (MCR) person search Application Program Interface (API) to search insurance applications using marketplace consumer PII. Data elements used for person search are first name, last name, city, state, zip, social security number. Date of birth, and phone number. The search criteria are not persisted.

ESDCU users are CMS employees and direct contractors. ESDCU is accessed in two ways. 1. The ESDCU appeals workers use the CMS Enterprise Portal and select the ESDCU application within that environment; they do not enter user credentials into ESDCU. Login credentials are entered into the CMS Portal and are managed by Enterprise Identity Management (EIDM). The EIDM has its own PIA about the information contained within it. 2. System Administrators access the ESDCU through the CMS Virtual Private Network (VPN); they log in using their CMS Enterprise User Administration (EUA) ID which has its own PIA for the information that it handles.

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

ESDCU maintains a list of known portal user IDs for use in the monthly user reconciliation process. Information about whether the IDs have been recently used is shared with the POC of each user group as part of the process.

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 content of the FFM and is not collected from the public.

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

ESDCU does not have secondary uses for the PII.

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.

The Privacy Policy section of the Individual Application contains information about the privacy and

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

Other

Government Sources

Within the OPDIV

Non-Governmental Sources

Public

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 FFE system. FFE will outline any processes for notification. Also, system users' access ESDCU through other CMS systems, EIDM and CyberArk/Exchange Operations Center (XOC). Those systems would notify individuals. For information obtained from EIDM, it is the responsibility of this system to provide individuals the option to opt-out.

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 FFE system. FFE will outline any processes for notification. Also, system users' access ESDCU through other CMS systems, EIDM and CyberArk/XOC. For information obtained from EIDM, it is the responsibility of this system to provide individuals the option to opt-out.

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 FFE system. FFE 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 FFE system. However, an individual can contact the FFE 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 FFE, 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.

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 Information System 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 are 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. Role-based training is provided to those with elevated privileges on a quarterly basis.

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-GRS2022-00090002, which states that records will be destroyed when no longer needed for business use, or according to an agency predetermined time or business rule. The DAA record schedule for HIX was approved by Office of the Archivist in June 2023.

ESDCU complies with GRS 5.1 and 5.2.

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

ESDCU is hosted at Amazon, AWS operates the data centers in alignment with Tier III+ guidelines 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.