US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

08/23/2016

OPDIV:

CMS

Name:

Exchange Operations Center

PIA Unique Identifier:

P-7500088-985404

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 Exchange Operations Center (XOC) is an operations center that monitors the systems that comprise the Federally Facilitated Marketplace (FFM), Enterprise Identity Management (EIDM), and Data Services Hub (DSH) Technologies. The XOC coordinates the processes and activities that focus on restoring service to any of these systems as quickly as possible using phone lines and mail servers after any incident that may disrupt these services. Specifically, the XOC monitors system performance and failed transactions along with any failed login attempts within the different system components.

The FFM operates as the Health Insurance Marketplace where states have chosen not to build their own Marketplace.

DSH help with verifying applicant information used to determine eligibility for enrollment in qualified health plans and insurance affordability programs. DSH will provide one connection to the common federal data sources (including but not limited to Social Security Administration, Internal Revenue Service, Department of Homeland Security) needed to verify consumer application information for income, citizenship, immigration status, access to minimum essential coverage, etc.

The EIDM allows the capability for a single user account for use to access the multiple systems that comprise the Federally Facilitated Marketplace.

The PII collected within XOC provides access to the FFM, EIDM and DSH in order to monitor the systems that comprise these technologies.

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

The Exchange Operations Center does not collect, maintain, or share public information. The center is a focal point for monitoring systems supporting FFM/EIDM/DSH and coordinates the processes and activities to restore any failed services. The XOC monitors system performance and failed transactions along with any failed login attempts within the different system components.

The XOC is not a health marketplace system, they are an operations center that views in real time the marketplace systems metrics and performance health. They review real-time feeds of system memory, disk and CPU usage. They are also able to note any failed transactions that are occurring with marketplace systems. The specific details and information of these transactions are held by each of the individual marketplace systems and not the XOC. The XOC communicates with those system maintainers to validate and resolve the alerts that they view through the system performance indicators.

The XOC does document and maintain records of the severity and time durations of all marketplace systems incidents. They also document identified root causes and remediation tasks. The XOC operations team share a shift log during team transitions that identify current status of activities that are occurring, for example, any outages or degradations within the marketplace that maybe occurring.

In order to grant access to monitor the Federally Facilitated Marketplace (FFM), Enterprise Identity Management (EIDM), and Data Services Hub (DSH) Technologies, the user must provide his or her user ID, password email, name and phone number.

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

The Exchange Operations Center does not collect, maintain, or share public information. The center is a focal point for monitoring systems supporting FFM/EIDM/DSH and coordinating the processes and activities. The XOC reviews and monitors system health and performance and is the central communication channel for FFM. All FFM system maintainers are directed to communicate with the XOC during any outages, maintenance, or degradations. The XOC is used for all teams to collaborate regarding the status of the healthcare.gov website. The XOC has an open bridge (24x7) which allows every team to communicate status and issues real-time. The XOC also manages and communicates healthcare.gov maintenance and testing schedules alerting CMS to the needs of vendors and required authorizations.

User credential (user ID, password, email, name and phone number) is used to gain access into FFM, EIDM and DHS in order to monitor system performance and failed transactions along with any failed login attempts within the different system components.

The PII collected within XOC provides the ability to monitor the systems that comprise the FFM, EIDM, and DSH. The PII collected within the systems that comprise FFM, EIDM, and DSH is covered under separate PIAs.

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

Phone Numbers

User ID and password

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

Employees

Only CMS employees and CMS contractors

How many individuals' PII is in the system?

500-4,999

For what primary purpose is the PII used?

User credential (email, name and phone number) is used to gain access into FFM, EIDM and DHS in order to monitor system performance and failed transactions along with any failed login attempts within the different system components.

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.

5 USC 301, Departmental Regulations

Are records on the system retrieved by one or more PII data elements?

No

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Email

Government Sources

Within OpDiv

Non-Governmental Sources

Private Sector

Identify the OMB information collection approval number and expiration date

N/A

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.

Individuals requesting access must sign an Acceptable User Agreements prior to account creation. Account request form must also be filled indicating name, email, phone number and access level needed. This form is reviewed and approved by the System information Security Officer (ISSO) prior to account creation.

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.

Potential user cannot 'opt-out' of providing their PII (email, name and phone number). This PII is needed to create a user account in order to perform their job duties and gain access into FFM, EIDM and DSH to monitor system performance and failed transactions along with any failed login attempts within the different system components.

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

Individuals requesting access must sign an Acceptable User Agreements prior to account creation.

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.

Account holders can contact the Access Control team via email.

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

In order to maintain the integrity, availability, accuracy, and relevancy of the PII, 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.

Under this process, outdated, unnecessary, irrelevant, and inaccurate PII is identified and deleted. The PII is available as needed, and is sufficient (minimum required) for the purposes needed. Only system administrators can create or modify PII. Activities of all users including system administrators are logged and reviewed by XOC System information Security Officer (ISSO) to identify abnormal activities if any.

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

Users:

Users monitor system performance and failed transactions along with any failed login attempts within the difference system components.

Administrators:

Administrators create the accounts for the users and modify account information if necessary.

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

Individuals requesting access must sign an Acceptable User Agreement prior to account creation. Account request form must also be filed indicating name, email, phone number and access level needed. This form is reviewed and approved by the System information Security Officer (ISSO) prior to account creation. XOC 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. 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 XOC ISSO to identify abnormal activities if any.

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.

XOC 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. 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 XOC ISSO to identify abnormal activities if any.

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.

Both Federal and Direct Contractor staffs who access or operate a Centers for Medicare and Medicaid Services (CMS) system are required to complete the annual CMS Security and Privacy Awareness training provided annually as Computer Based Training (CBT) course. Contractors also complete their annual corporate security training.

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

CMS employees and direct contractors with privileged access are required to complete role-based training and meet continuing education requirements commensurate with their role. Other training avenues such as conferences, seminars and classroom training provided by CMS/HHS is available apart from the regular annual training.

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.

Records Association (NARA), General Records Schedule (GRS) 20 states that XOC will destroy/delete when 7 years 6 months, 10 years 6 months, or 20 years 6 months old, based on the maximum level of operation of the Certification Authority, or when no longer needed for business, whichever is later and GRS 24 states that XOC will delete/destroy when agency determines they are no longer needed for administrative, legal, audit or other operational purposes.

System Administrators review user accounts at least semi-annually to remove user PII if access is no longer required.

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

XOC 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. 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 XOC ISSO to identify abnormal activities if any.

XOC is located at a secured facility. Physical controls are in place such as security guards to ensure access to the buildings is granted to only authorize individuals. Identification of personnel is checked at the facility.

XOC is built using industry best practices and independently reviewed against Federal Information Security Management Act (FISMA) and National Institute of Science and Technology (NIST) Security and Privacy controls to ensure technical, operational, and management controls are properly applied.

Personally Identifiable Information (PII) in XOC is secured administratively by ensuring that the system goes through the Assessment and Authorization (A&A) process, and all documentation is submitted to the Information Security & Privacy Group (ISPG) that supports the system and to comply with Federal Information Security Management Act (FISMA) regulations.