# US Department of Health and Human Services

## Privacy Impact Assessment

### Date Signed:

09/12/2016

### OPDIV:

CMS

### Name:

Opportunity to Network and Engage

**PIA Unique Identifier:**

P-4815915-185726

**The subject of this PIA is which of the following?**

Minor Application (stand-alone)

**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 CMS Opportunity to Network and Engage (zONE) application is a collaborative online platform for State-based Marketplace (SBM) exchanges, insurance agents, and business and technology teams to connect, communicate, and share information. This sharing of information such as, documents, resources, and best practices, is to create a learning culture for the advancement and further success of the SBM exchanges.

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

zONE stores the following information passed by CMS' Enterprise Identity Management (EIDM) system after a user registers in that system and is authenticated/provided permission to access zONE: EIDM ID and password, EIDM user name (user's first and last name), and on-file email address. zONE may also store (optional) user-provided profile photos and organization names.

zONE collects and shares content such as documents, events and "Wikis" (explained below) which are community related content. As part of creating content, users are allowed to: (1) upload standard files such as .doc, .xls, and .pdfs; (2) create text for title and description, and (3) enter Uniform Resource Locators (URL).

Wikis are more complex documentation/ content that can be edited by multiple authorized members and revisions can be tracked.

In addition, zONE may store information pertaining to the internal operations of a network or computer system, including: network and device addresses; system and protocol addressing schemes implemented at an agency; network management information protocols, community strings, or network information packets; or zONE may store security management information for SBM exchanges or the Federal-facilitated Marketplaces (FFM), including security information on protection during operations.

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

zONE allows users to create content such as documents, events and 'Wikis' (explained below). As part of the content, users may also: (1) upload standard files such as .doc, .xls, and .pdfs; (2) create text for title and description, and (3) enter Uniform Resource Locators (URL). Wikis are more complex documentation/ content that can be edited by multiple authorized members and revisions can be tracked.

The documents and other information is used/shared between the users to provide examples of how one SBM exchanges may present information to consumers, how one SBM exchanges designed their website for the public to use, and/or the method for providing customer service or setting up a SBM exchange.

All content within zONE is stored until a decision is made by the Business Owners to delete or remove. Any content that is posted in zONE is subject to removal if it does not abide by the HHS Rules of Behavior as explained in House Rules within zONE.

Other information that zONE users may upload and store is information pertaining to the internal operations of a network or computer system, including: network and device addresses; system and protocol addressing schemes implemented at an agency; network management information protocols, community strings, or network information packets; or zONE may store security management information for SBM exchanges or the Federal-facilitated Marketplaces (FFM), including security information on protection during operations.

After a user registers in the EIDM system and is authenticated/authorized to access zONE, zONE will access the EIDM user name, EIDM ID and password and email address. Other information a user may upload, as an option, are a profile photo and organization information. User information is retained/accessed by zONE for as long as the user requires or wants access or subject to employment.

**Does the system collect, maintain, use or share PII?**

Yes

**Indicate the type of PII that the system will collect or maintain.**

Name

Photographic Identifiers

E-Mail Address

Other: organization name, user credentials: user ID and password, network and device addresses

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

Employees

Business Partner/Contacts (Federal/state/local agencies)

**How many individuals' PII is in the system?**

500-4,999

**For what primary purpose is the PII used?**

PII is used to create/register a user's zONE account in order for the community of users to communicate with one another within the collaborative application.

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

No Secondary Use

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

Affordable Care Act. Title 42 U.S.C. 18031, 18041, 18081—18083 and section 1414 and 5 U.S.C. 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

Online

**Government Sources**

Within OpDiv

State/Local/Tribal

Other

**Non-Governmental Sources**

Private Sector

**Identify the OMB information collection approval number and expiration date**

OMB No.0938-1236 Expiration Date: 04/30/2017

**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.**

User access for CMS zONE is through the registration process of EIDM, another CMS system. EIDM informs the user that the PII is being collected. There is a "terms and conditions" page that describes the collection and use of PII. New and returning users are presented with this page and they must click "I agree" to move forward with system access. The information provided to EIDM for registration is managed by EIDM and subject to the EIDM PIA.

**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.**

In order to use the zONE collaboration website, a user’s EIDM user credentials must be provided. Users do not have the option to opt out of providing this information based on the nature of the website to facilitate collaboration and information sharing.

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

Since access to zONE is controlled by EIDM access, zONE doesn't notify the users. EIDM informs the user that the PII is being collected. The PII provided to EIDM for registration is managed by EIDM. There is a "terms and conditions" page, that describes the collection and use of PII, which both new and returning users are presented with, and they must click "I agree" to move forward with system access.

**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.**

As a part of the community based collaboration environment, users will only have access to PII provided in the user profiles. If a user believes this information has been accessed or used in an inappropriate manner, they have the ability to contact the Federal Exchange Program System (FEPS) helpdesk: CMS_FEPS@cms.hhs.gov, or 1-855-CMS-1515.

The FEPS helpdesk will open a file and review the situation to resolve the individual's concerns.

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

Authentication to zONE is managed via EIDM. CMS zONE Business Owners grant and revoke users' zONE access. When a user successfully authenticates in EIDM, the user's information is passed to zONE. When a user no longer requires access to zONE, CMS zONE Business Owners remove the access to the zONE application in the user's EIDM profile. As a part of the community based collaboration environment, users will only have access to PII provided in the user profiles.

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

**Users:**

Users have access to search and view other zONE user profile information, which includes name and organization and/or profile picture if provided, in order to communicate and share content.

**Administrators:**

Users with administrator role may access to the name, profile picture and email addresses in order to support role based authorization which is internal to the zONE.

**Contractors:**

Users may be direct contractors that support the system by managing the software, hardware and other backend systems that support the zONE.

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

The CMS zONE Business Owners have the approval authority for authorizing role based access to zONE via EIDM (Enterprise Identity Management). Users of the zONE application may request access to desired communities within zONE and the Administrator will either approve or deny the requestor’s access to the community based on justification provided by the requestor. After users receive appropriate approval to access zONE, they can also request for community creation within zONE. The Business Owner reserves the right to create the community based on requestor’s justification. If the request is approved by the Business Owner, a community will be created and the requestor will be assigned the Administrator role for that community. Access can also be granted as an Administrator based on the justifications identified by the CMS zONE Business Owners.

**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.**

The system restricts access to PII depending on the role granted to the user. Users without the appropriate role cannot see the PII. Depending on the justification provided by the requestor, the Business Owner can grant the roles of Administrator or User from a drop down menu. The Administrator and User roles are created in zONE with a specific set of pre-approved permissions for each role. These approved permissions determine if the user can see first name, last name, and/or email address (PII). If the requestor is denied the requested Administrator role, then the requestor will have user level permissions selected from the drop down menu and the system will restrict the user from viewing email addresses. System administrators have the ability to provide additional access within the zONE application if requested and authorized by the CMS zONE Business Owners.

**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.**

The zONE team is provided with Annual Security Training, which includes computer-based training in their responsibility to protect sensitive information. This training is provided by CMS as well as the contractor organizations for compliance with CMS guidelines. The training, including annual and refresher Security and Privacy Awareness training and access recertification, is provided on an annual basis and at start up for new hires.

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

Once a user has access to zONE, they will be able to view the CMS zONE 101 training materials, "House Rules" documents and user manuals which provide Rules of Behavior and other guidelines for using CMS zONE.

**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 data will be stored indefinitely until NARA determines the appropriate records schedule.

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

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, role-based access for developers and administrators. For example, if a user is granted the role of zONE user, then the controls embedded in the system allow him to see only information that is allowed for “User role”. If the user is approved to have “Administrator role”, then the user will be able to see the name and the email ID as intended by the system design.

The technical controls in place are firewalls that prevent unauthorized access, encrypted access when users obtain the EIDM authentication (approval) to log into the application and a tiered system architecture which means users can only log into the application but not into any test environment and the testing and active applications are not joined together.

The physical controls in place are as follows: the zONE system is hosted in the CMS HP (Hewlett Packard) Virtual data center. The data center is located in a special facility in Tulsa, OK. It has exterior security controls- use of security cards and pass codes, security guards and the zONE maintenance team accesses the zONE system by CMS authentication and access controls by using security tokens and user credentials.