US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

04/07/2016

OPDIV:

CMS

Name:

Virtual Audit Management System

PIA Unique Identifier:

P-9020203-208894

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.

Agency

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.

N/A

Describe the purpose of the system.

As part of the Affordable Care Act (ACA), the Virtual Audit Management System (VAMS) was created to provide an audit management tool for the CMS Center for Consumer Information and Insurance Oversight (CCIIO) Group was created to manage the analysis, audits, examinations, form filings, rate review analysis and the associated documents and work papers of Qualified Health Insurance Providers (QHPs) participating in the Federally-Facilitated Marketplaces (FFM).

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

VAMS collects documentation from QHPs to allow for the audit and additional review of QHPs in accordance with the Affordable Care Act (ACA). The documents include details of QHP operations, such as operations and maintenance manuals, insurance form filings and insurance rates documentation.

To access VAMS, there are a limited number of registered users that input a user ID and password. User IDs and passwords are created in the Hewlett Packard Enterprises Virtual Data Center 1 (HPE VDC1) Active Directory system. The users must provide their name, email address and telephone number to create a user ID and password.

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

VAMS is an audit management tool that allows the CCIIO to create and manage the analysis, audits, examinations, form filings, rate review analysis and the associated documents and work papers of QHPs. The information is stored temporarily.

Additionally, to access VAMS, users input a user ID and password. This information is maintained for as long as the user requires access for job functions. User IDs and passwords are created in the HPE VDC1 Active Directory system and are subject to the HPE VDC1 PIA.

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

Other - User credentials- user ID and password

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

Employees

Vendor/Suppliers/Contractors

How many individuals' PII is in the system?

100-499

For what primary purpose is the PII used?

PII is required to identify VAMS system users and allow access to VAMS.

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

Not applicable.

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

5 USC Section 301, Departmental Regulations

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 Program

SORN is In Progress

Identify the sources of PII in the system.

Online

Government Sources

Within OpDiv

Non-Governmental Sources

Other

Identify the OMB information collection approval number and expiration date

Not applicable for the creation of 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.

To get into the VAMS system, a user must first log into the HPE VDC1 system. At that logon, there is notification that the user is logging into a government computer system. Since the user is first logging into the HPE VDC1 system, that system is responsible for notifying the user that PII is being collected.

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.

Users cannot opt-out of collection or use of PII (their user credentials) because it is required to access the VAMS system.

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

Major changes to the VAMS system, including a change in authentication mechanism for user credentials, will include multiple communications to the users following the VAMS Release and Version Management Plan. This plan includes emailing individuals with PII in the system to inform them of major changes that will take place.

Additionally, since the user is first logging into HPE VDC1, that system is responsible for notifying the users of any changes to that system's parameters.

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.

VAMS system users can contact the HPE VDC1 Help Desk with any concerns regarding their user credentials. They can contact via email or telephone.

They can also contact the CMS Information Technology (IT) Help Desk to report PII concerns related to the HPE VDC1 system. A user can either email or call the Help Desk. The Help Desk may engage HPE VDC Security Operation Center (SOC), if additional support or investigation is required for resolution of the concern.

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

There are automated processes within the VAMS system that ensures that a user's ID, email address, and name are accurate. This process includes the implementation of a tool that emails a user when his or her password will expire.

Availability of PII is managed by automated tools at the HPE VDC1 that automatically notify engineers when the system is offline.

Quarterly audits of the business requirements and user accounts ensure integrity of the user accounts by reviewing the status of users and removal of inactive accounts.

PII accuracy is maintained by automated emails to users when their password is set to expire and if it has expired. Relevancy is reviewed through a quarterly audit of system requirements as they related to the relevancy of PII captured (i.e. are user names and email addresses still required).

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

Users:

Users perform the functions of VAMS. As such, they must know each other's names and email addresses in order to complete audits and communicate with each other.

Administrators:

Administrators need to be able to update users' information, including name, email address, and phone number.

Contractors:

Contractors are contracted by CMS to perform audits of Health Insurance Providers. As such, they must know each other's names and email addresses in order to complete audits and communicate with each other.

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

Administrative controls within the system ensure that only the users with the proper permissions have access to PII within the system. Specifically, this user group (users) contains all users within the system. Users who have not been granted the role of 'User' cannot access PII within VAMS. Access is to PII is granted based on the user's role following the principles of minimum necessary and least privilege

Access to the “'User”' group is granted by System Administrators. This group is audited quarterly.

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.

Access is to PII is granted based on the user's role following the principles of minimum necessary and least privilege. Administrators must approve all system access and re-certify that access within every 365 days. Only administrators may change PII within the system. All actions are logged.

Technical controls for this access are provided through the Active Directory maintenance tool within HPE VDC1. Authority to use this tool is only given by the HPE VDC1 administrators.

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 support contractors with CMS accounts must take the annual Security and Privacy Awareness training provided by CMS on an annual basis. Users acknowledge successful training after passing a test at the end of training and the system verifies completion. Included in the training is education about how to properly handle sensitive data.

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

There is no training above and beyond the CMS regular Security Awareness and Privacy 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.

All PII will be retained for as long as necessary or until system retirement. After system retirement data destruction will be handled per the established CMS guidelines. This will include deletion of data from physical drives, and formal documentation of data destruction with signed confirmation by the contractor and business owner.

Per National Archives Record Association approved record Disposition Authority, GRS 24, item 13a1: 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.

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 HPE VDC1 system, periodic review of users and deletion of non-active accounts, role-based access for developers and administrators.

The technical controls in place are firewalls that prevent unauthorized access, encrypted access when users access VAMS and computer system controls that prevent users without administrative or developer access to log into a test environment. The test environment and usable application are not joined together.

VAMS is hosted in the HPE VDC that employs physical controls and monitoring to restrict physical access and ensure the security of doors; the efficacy of heating and air conditioning, smoke and fire alarms, and fire suppression systems; and by employing cameras, fencing and security guards.