US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

07/18/2017

OPDIV:

CMS

Name:

DXC-VDC1

PIA Unique Identifier:

P-2107251-732503

The subject of this PIA is which of the following?

General Support System (GSS)

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.

Not Applicable

Describe the purpose of the system.

Hewlett Packard Enterprise (HPE) Virtual Data Center (HPE VDC1) is a General Support System (GSS) which supports Centers for Medicare & Medicaid Services (CMS) Major Applications (MA), providing Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) functions. The Major Applications are the communication platforms and websites that CMS uses to communicate internally and externally.

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

The HPE VDC1 does not directly collect, maintain, or disseminate any information, but provides infrastructure support for CMS MA.

For HPE VDC1 system support staff to operate the functionality of the system, they must create an account with their name and email address. The users create user credentials (User ID and password) for access to the system.

The Major Applications that are hosted by the HPE VDC1 may collect, maintain or share information, including PII. As such, it is the responsibility of those applications to secure the PII. For information on the PII potentially housed in those systems, it is necessary to review the Privacy Impact Assessments (PIA) for those systems. HPE VDC1 does not access the applications. The Major Applications that HPE VDC1 hosts are listed below:

TWS Tivoli Workload Scheduler; CPMS CO-OP Program Management System SERTS State; Exchange Resource and Tracking System; SERVIS Stat Exchange Resource Virtual Information System zONE; Opportunity to Network and Exchange; ERR Enrollment Resolution and Reconciliation; VAMS Virtual Audit Management System; HIOS Health Insurance Oversight System; CMMI CMS Innovation Learning and Diffusion; CALT Collaboration Application Lifecycle; Tools EDGE Enrollment Data Gathering Environment; SHOP Small Business Health Options Program; MIDAS Multidimensional Insurance Data Analytics; System Adobe Adobe LiveCycle (Digi Docs); EIDM Enterprise Identity Management;RBIS Rate and Benefits Information System;FM Financial Management; PM Plan Management; EFT Electronic File Transfer; VM Vendor Management; LMS Learning Management System; DSH Data Services HUB; ASP Average Sales Price; E&E Eligibility and Enrollment; EPS Eligibility Payment System; MLMS Marketplace Learning Management System; MQM Marketplace Quality Module; FM Tower OPERA OA & QA; PP Payment Processing

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

HPE VDC is a GSS supporting CMS Major Applications (MA) by providing infrastructure and platform support services. The infrastructure (IaaS) provided to CMS includes the hardware and processing software on which the MAs operate. The platform services (PaaS) are the networking components, software storage and programming capabilities that CMS uses to configure the applications. CMS uses the MAs to communicate internally and externally. The information within those systems is not within the boundary of the HPE VDC1.

HPE VDC1 system support staff, CMS employees or contractor, enter their name and email address which is used to authenticate the individual and create a user account. The user credentials, user ID and password, allow access into the HPE VDC1 system for administration and maintenance of the system. The credentials are stored for the term of employment of the user or for the job function.

If a system user leaves or changes positions, their user credentials are disabled or eliminated from the system.

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

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?

HPE VDC1 uses CMS employee or contractor name and email address to authenticate the individual and create a user account. The user credentials, user ID and password, allow access into the HPE VDC1 system for administration and maintenance of the system.

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

There are no other secondary uses of PII.

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.

09-70-0538, Individuals Authorized Access to CMS Computer Services

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Online

Government Sources

Within OpDiv

Non-Governmental Sources

Private Sector

Identify the OMB information collection approval number and expiration date

Not applicable for user credential information to support system functions.

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.

When the CMS employee or contractor system users log into HPE VDC1, they are presented with a login page that states that they are accessing a CMS computer system and that their credentials are 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.

There is no option to "opt out" of providing user credentials (PII) because it is required to access the system in order to perform job duties.

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

If a major system change was to be implemented within the HPE VDC1, the users would be notified via email and the login banner would include additional information. The CMS employee or contractor system users are utilizing implied consent since access to HPE VDC1 is dependent on inputting user credentials to access the system.

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.

A system user, CMS employee or contractor, can contact CMS IT (information technology) 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.

The data integrity, availability, accuracy and relevancy of the the PII (system user credentials) used to access HPE VDC1, is accomplished by the following methods:

The CMS employee or contractor system users can correct their own user credentials within their own account, or administrators can correct this for them. Administrators also run monthly reports to determine any discrepancies or problems, such as eliminating user credentials for inactive system users or reviewing the access permissions of system users to make sure that users are only accessing system tools required for their job functions, they can then take steps to make any corrections.

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

Administrators:

System Administrators have access to user credentials, PII, to provide system operations and maintenance support.

Developers:

Developers do not normally access PII but may need to access it to perform updates or other system changes, or operations and maintenance support.

Contractors:

Contractors, in their roles as either Administrators or Developers, may have access to PII to perform the functions of those positions.

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

To determine which system users have access to PII, HPE VDC1 applies the principle of least privilege as a Role Based security when granting security access rights. All security access for any user is requested and approved before being granted.

For planning, approving, and auditing, HPE VDC1 utilizes a Roles and Responsibilities matrix to review and track what resources are accessible. A monthly audit is performed for system accounts and quarterly user driven validation of accounts is required. New HPE VDC1 team members are processed through an onboarding process that defines their role and all information and approvals are archived in a trackable service request.

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 controls that are in place include the monitoring and approval of access requests via a service request ticket requiring an authorized Manager's approval and role-based access so that users are restricted to only the resources needed to perform their job functions. HPE VDC1 applies the principle of least privilege using Role Based Access Controls (RBAC) and each user is assigned a Role which restricts the user to only the resources and servers needed to perform their job functions.

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.

Security Awareness and Privacy training is required and provided to the system users, including CMS contractors, on an annual basis. CMS employees and support contractors with CMS accounts must take the annual Security and Privacy awareness training provided by CMS. 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).

Additional Role-Based training is taken by CMS employees. Hewlett Packard Enterprise (HPE) personnel, must complete the HPE Corporate Compliance and HPE US Public Sector training which includes role based access topics.

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 will be retained and destroyed in accordance with published records schedules of CMS as approved by the National Archives and Records Administration (NARA):

Delete/destroy when agency determines they are no longer needed for administrative, legal, audit or other operational purposes (Disposition Authority: GRS 20, Item 1).

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

HPE VDC1 is managed by Hewlett Packard Enterprise (HPE). The physical controls that are in place include security guards, video monitoring and the use of security cards for access.

The technical controls in place are: firewalls that prevent unauthorized access, encrypted access when users log into the application, a tiered system architecture where users can only log into the application but not into any test environment simultaneously, anti-virus technology and intrusion detection systems (IDS) and intrusion prevention systems (IDS).
From an administrative standpoint, HPE VDC1 applies the principle of least privilege using Role Based Access Controls (RBAC) and each user is assigned a Role which restricts the user to only the resources and servers needed to perform their job functions. Vulnerability scans and security compliance reviews are conducted monthly to examine the system and correct any issues that are found.