US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

03/18/2016

OPDIV:

OS

Name:

HHS Email as a Service

PIA Unique Identifier:

P-1517605-175615

The subject of this PIA is which of the following?

Major Application

Identify the Enterprise Performance Lifecycle Phase of the system.

Implementation

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)?

No

Indicate the following reason(s) for updating this PIA.

Significant System Management Change

The Department of Health and Human Services (HHS) Email as a Service (EaaS) system has had additional components added to support Enterprise Mobility Management (EMM) of mobile devices.

Describe in further detail any changes to the system that have occurred since the last PIA.

EaaS has implemented additional virtual servers which provide for EMM of mobile devices. These servers provide a management console and methodology for the enforcement of policy, and serve to provide a communication path between the on-premise infrastructure components and the IBM Fiberlink MaaS360 cloud components, which are authorized under the Federal Risk and Authorization Management Program (FedRAMP) process.

Describe the purpose of the system.

The HHS has established EaaS as a cloud computing Software as a Service (SaaS) solution for email, collaboration, and communication tools which leverages the Microsoft Government-only and IBM Fiberlink MaaS 360 cloud. The cloud services align with the descriptions provided by the National Institute of Standards and Technology (NIST) in Special Publication 800-145.

The primary purpose of EaaS is to leverage FedRAMP approved Government Community Cloud (GCC) solutions to obtain improvements in continuity operations, collaboration, efficiency, agility, innovation, and cost savings, for email and office productivity services previously provided by its enterprise email applications and existing collaboration solutions, including the asset management of mobile devices, through the registration of the devices with the EMM Server by support personnel, which allows for the management of configuration settings on the device through the application of policy, such as creation of a secure encrypted container which is used for storage of HHS information, enforcing restrictions on software installation, enforcing the use of a secure browser, enforcement of security policy on the device, and remote wiping of the secure contents on the device.

Information from the Email and EMM components may be used to ensure devices are compliant with HHS policies and to support HHS Incident Response processes by generating reports containing information such as mail recipient, mail sender, delivery confirmation, subject, mobile device identifier, mobile device policy and configuration settings, and provide for the sanitizing of secure containers on the mobile devices.

Reports are generated on a periodic basis, typically monthly, to comply with Federal continuous monitoring requirements and describe the number of devices registered with EMM, by assigned user, model and type, software versions, last connection of the device to the management server, and the HHS Operating Division to which they are assigned. EMM Incident Response reports can also be referenced against email reports in certain circumstances to determine if email was delivered to a mobile device.

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

The e-mail system does not collect or request specific PII data; however, there is a possibility of the exchange of PII data between individuals or groups of individuals through the transmission of e-mail messages. These messages could be stored for retrieval in a user's mailbox or personal archives indefinitely as well as retained in storage arrays for 14 days which is the HHS e-mail retention policy.

E-mails are transmitted between HHS employees for normal day to day business operations but PII data is never explicitly collected or used by the system (i.e., there are no forms or fields for PII collection, and PII collection is not the explicit purpose of the system).

The EaaS system itself does not include an Active Directory server within it's Authorization to Operate (ATO) boundary, but interconnects to the existing Active Directory infrastructure in order to manage and authenticate users' access to their mailboxes and to register mobile devices to a user. As a result, Active Directory field data requirements are managed by the General Support System rather than the EaaS system, but EaaS will synchronize with Active Directory and may maintain this information. This information typically includes User Principal Name, first, middle, and last name, organization, office number, email address and phone number. Additional data types required by the EMM component include device identifiers for the mobile devices enrolled in the service. EMM also monitors device status through identification of the device model, operating system version installed, policy applied, connectivity status and device owner as pulled from the General Support System Active Directory.

This information may be shared with the Program Manager, System Administrators, Incident Response Team members, and Help Desk Support team members to assist in performing their duties and portions of this data may be manually entered in the help desk ticketing systems.

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

EaaS is a Major Application (MA) supporting the transfer of messages among users of the system; messages can be sent from HHS staff members to other HHS staff members or externally to other e-

mail users; that is to say, this e-mail system will have all the capabilities expected of other e-mail systems. Data processed on the EaaS is considered Controlled Unclassified Information (CUI).

EaaS stores or passes PII data that could be contained in e-mails between individual users sending and receiving e-mails on the system. Those e-mails are stored on a service provider's cloud servers. Users would also have the ability to save e-mails in local archives on their individual workstations.

In most cases, the submission of PII is voluntary, but required in order to receive benefits, serve as an employee of HHS, etc. The nature of the data collection will vary widely along with the underlying business practice.

Note that under some analyses, the use of an e-mail service would be considered not to involve the collection, maintenance, use, or sharing of PII, but to be the use of a "common carrier" that merely transmits the PII in the service of other business practices and applications.

The EMM component provides for the asset management of mobile devices such as smartphones and tablets, which have been issued by the Operating Division and must then be registered with the EMM servers by support personnel such as System Administrators or Help Desk Personnel, or in accordance with HHS registration procedures and instructions provided to the users, which install an agent which manages connection and periodic synchronization to the server . A self-registration process using instructions provided by the support team is also available. EMM manages the application of configuration settings and security policy, enforces the use of a secure, encrypted container for HHS information, and is capable of disabling or sanitizing registered devices upon connection to the server.

EMM also monitors device status through identification of the device model, operating system version installed, policy applied, connectivity status and the device owner as pulled from the general support system Active Directory.

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

Device Identifiers

Any information a user chooses to include in an email message that may contain unspecified PII

Active Directory credential information (UID) to allow for mailbox synchronization and email delivery

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

Employees

Public Citizens

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

Vendor/Suppliers/Contractors

Patients

Any information a user chooses to include in an email message that may contain unspecified PII data.

How many individuals' PII is in the system?

1,000,000 or more

For what primary purpose is the PII used?

The uses of PII would be as varied as the functions and activities of HHS. Uses could include determination of benefits; health care payment, treatment or operations; conduct of health-related research; internal administrative and human resources functions; conduct of background checks; disciplinary actions; certification of health care service providers; or any of dozens of other activities HHS conducts. Active Directory credential information (primarily User Principal Name, userID and authenticator) is used by the system for authentication purposes only.

The EaaS system may also access additional information stored in the General Support System's Active Directory such as electronic address information, but this information is defined by the GSS, and not needed by the EaaS system.

The EMM component will use mobile device identifiers for asset management and configuration of mobile devices assigned to an individual and the application of group policy to that device.

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

No root-level or administrative users will have access to all the PII in this system. It is conceivable that HHS will employ some form of data loss prevention or discovery tool to identify PII contained in e-mails for purposes of complying with a discovery request or evaluating its privacy and security practices.

A secondary usage for PII in the EMM component is for incident response support. The device information, including assigned user, would be compared against other response reporting mechanisms such as email records, continuous monitoring reports, and policy compliance management reports to assist in categorization, reporting, and remediation of information security incidents.

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

Not Applicable. Information use and disclosure over this system is governed by the laws and regulations of the individual business practice that this system is used to conduct.

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

Hardcopy

Email

Online

Other

Government Sources

Within OpDiv

Other HHS OpDiv

State/Local/Tribal

Foreign

Other Federal Entities

Other

Non-Governmental Sources

Public

Commercial Data Broker

Media/Internet

Private Sector

Other

Identify the OMB information collection approval number and expiration date

Not Applicable

Is the PII shared with other organizations?

Yes

Identify with whom the PII is shared or disclosed and for what purpose.

Within HHS

User email address may be shared as part of normal communication. Content of email varies with business function. Mobile Device Assigned User, Device identifier information, usage information and configuration information may be shared with the HHS OS Incident Response Team to support incident response investigations.

Other Federal Agencies

User email address may be shared as part of normal communication. Content of email varies with business conducted. EMM device information is only shared with other federal agencies in incident response circumstances.

State or Local Agencies

User email address may be shared as part of normal communication. Content of email varies with business conducted. EMM device information is typically not shared with State or Local Agencies, but minimal device identifier and assigned user might be shared with such agencies in incident response circumstances such as a lost or stolen mobile device.

Private Sector

User email address may be shared as part of normal communication. Content of email varies with business conducted. EMM information is not shared with the private sector other than the partner cloud service providers.

Describe any agreements in place that authorizes the information sharing or disclosure.

The agreements governing information exchange will vary with the business functions and purposes of exchanging e-mail. Memorandum of Understanding and Information Sharing Agreements are used between EaaS and CMS.

Describe the procedures for accounting for disclosures.

The HHS EaaS may be required to make such disclosures in the event that discovery is required pursuant to a legal action; at the request of the Secretary; if needed to respond to public health or other national emergencies; or to investigate privacy or security breaches. Such requests can be performed by an approved System Administrator through the use of a mail query function submitted via the system interface portal, which allows for mailbox searches based on predefined criteria.

An accounting of responses for such disclosures is managed through the existing management processes within HHS/OS. This process is the same for Email as a Service as well as EMM.

Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.

The processes will vary along with the underlying business processes and practices that the use of e-mail and EMM is supporting.

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.

No PII data is specifically collected or used through the use of an e-mail system; therefore, there are no notifications to users about PII data and no consent obtained from individuals. Obtaining consent and/or providing notification is part of the business processes underlying the use of an e-mail service.

Any PII data contained in e-mail messages is only shared with the user(s) to whom the e-mail is sent.

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

No PII data is specifically collected or used through the use of an e-mail system; therefore, there are no notifications to users about PII data and no consent obtained from individuals. Obtaining consent and/or providing notification is part of the business processes underlying the use of an e-mail service and the mobile devices managed by EMM.

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 a Department-wide process. Individuals would not be likely to discover concerns through the use of PII in the e-mail system, but through the underlying business processes. Avenues for redress would include contacting the operations centers, help desks or customer service providers of those individual business operations. Members of the public could also avail themselves of the Freedom of Information Act (FOIA) or Privacy Act redress services.

For issues with PII detected by HHS staff members, individuals could also report suspected fraud, breaches, or other issues to the Computer Security Incident Response Center (CSIRC) or to the business process owner.

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

Data integrity is maintained at the level of the business process, or through maintenance of the

applications that support business processes. Review of PII in e-mail systems would not be efficient or appropriate. Email message headers and attachments may be reviewed and sorted through the use of predefined search options, including key-word search, to support security incident response, data loss prevention, or e-discovery. Periodic reviews of EMM reports containing user ID and device identifiers are used to ensure that devices are issued, configured, and protected as required.

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

Users:

To retrieve and use e-mail messages for day to day work functions.

Administrators:

To operate and maintain the e-mail system and the mobile device management servers and enrolled mobile devices.

Contractors:

Specifically authorized contractors serving as System Administrators will have access to Active Directory credential and mobile device identifier information for performing synchronization and testing duties required in the normal operation of the system.

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

Only users (i.e., those authorized to send and receive e-mails) and administrators are able to access the contents of e-mails. The cloud service providers will be prevented from accessing contents of e-mails using encryption standards, and accessing the content will not be part of the services provided.

HHS employees and contractors that have completed the personnel screening process and corresponding forms and documents are provided email accounts as part of their employment package, and these mail accounts are accessed through EaaS. EaaS Administrators are approved by the Program Manager, and must complete necessary Network Access Request forms and training to obtain the elevated privileges required for administrative duties. The EaaS administrator must also register and request access, and sign corresponding NDAs, to the Microsoft Administration Portal and the IBM Fiberlink MaaS360 interface for access to the management interface for the cloud-based components.

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.

This is a standard e-mail system, and e-mails are sent from user to specified recipients. Other parties (system administrators, contractors, users not party to a specific communication, etc.) will not have access to e-mails not specifically addressed to them. Cloud providers in particular are not expected to have any access to the content of transmissions.

HHS EaaS system administrators with the appropriate permissions, who have signed Rules of Behavior and performed the required training, are able to access the mobile device identifiers and the contents of e-mails, for authorized purposes such as e-discovery or detection of breaches.

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.

All users are required to complete annual Information Security Training and Privacy Awareness Training.

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

User will be provided training regarding the basic concepts of accessing email and collaboration services offered by the EaaS cloud-based solution. EaaS Administrators are required to complete training in Security Incident Response, Contingency Planning and Operations, and Role-Based training. Help desk support staff are trained in mail support and mobile device registration tasks.

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.

User can archive messages containing PII data on their workstation or in their mailbox indefinitely. Otherwise, the data retention policy on the storage arrays is 14 days. If a user deletes a message, at which time it is moved to the Deleted Items Recovery folder for 14 days. After this period, the deleted mail is stored in a purge folder for 14 days, during which time only authorized administrators can access it. Mobile Device identifiers used by the EMM component will be maintained until the National Archives and Record Administration retention schedule has been determined by the OS Records Management Office.

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

EaaS implements security controls to protect PII, as defined by OMB mandates, the Federal Information Security Management Act (FISMA), and NIST Special Publications (SP) 800-53, 800-37, 800-122, NIST Federal Information Processing Standards (FIPS) 200, 201, 199, 197, 140-2, and other associated documents as outlined by Federal Risk and Authorization Management Program (FedRAMP) (www.fedramp.gov). This includes achieving and maintaining an Authority to Operate (ATO)

PII will be secured within the system through the use of administrative controls in the form of:
Mandatory security awareness and privacy training for all users;
Role-based training for privileged users;
Personnel screening as required by HHS;
Completion of contractual agreements and Rules of Behavior;
Users can encrypt email traffic, including those containing PII, in accordance with applicable HHS policies.

Technical controls include:
Role-based access controls based on Active Directory permissions to obtain authorized access to the system. All user login will be logged, with auditing performed as part of the EaaS Continuous Monitoring program.
Spam and email content filtering
Anti-malware software installed on EaaS servers
FIPS 140-2 compliant encryption of data in transit
Restricted access to the GCC through the HHS Trusted Internet Connection (TIC) Access Points
Information Flow Control through the use of firewalls, Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Security Information and Event Management (SIEM), Data Loss Prevention (DLP) and Continuous Data Protection (CDP) policy that allows for direct remote OpDiv administration
Non-repudiation through support of digital signatures and encrypted email, using PIV and other types of digital certificates.

Physical controls include:
Hosting within data centers which control and monitor physical access to the system components, including visitor control and auditing of access records.
Protection of power equipment and cabling, transmission medium, output devices and use of emergency power and shutoff systems as well as fire and water damage protection.