US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

08/06/2014

OPDIV:

OS

Name:

HHS Information Technology Infrastructure Operations Unified Communications System

PIA Unique Identifier:

P-2114468-080400

The subject of this PIA is which of the following?

Major Application

Identify the Enterprise Performance Lifecycle Phase of the system.

Planning

Is this a FISMA-Reportable system?

No

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?

New

Does the system have Security Authorization (SA)?

No

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

Describe the purpose of the system.

The UC infrastructure will reside on the Information Technology Information Office (ITIO) network and be designed for redundancy, scalability and interoperability.
The goals for this system is to implement a leading edge Unified Communications (UC) solution that includes Instant Messaging (IM), Presence Information, Telephony, Video Conferencing, Web Conferencing and Data Sharing for ITIO customers and provide Life cycle Management to comply with HHS policies and centralize management of the UC Solution. This is a telephony system in which the calls and voice messages features can be used and accessed from anywhere with a dial tone. The communication system itself cannot be used to contact or receive messages from another system from outside of HHS.

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

The type of information that is collected and maintained in the system includes:
Call Detail records (CDR) (information about each call, time, duration, calling party and party called, as well as technical call quality elements);
Voicemail messages;
Instant Messages;
Meeting IDs;
Personal Identification Numbers (PINs) (exclusively configured by end users to access hosted meetings); and
Active Directory information (user name, user ID, telephone number and email address).

In the event there is a PII incident, the incident response process will be followed. Per HHS Security Standards and Policy, users are educated regarding policies on disposal of PII. The user is required to delete this information and notify the sender this has taken place and the user must be retrained on HHS Security Standards and Policy.

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

The UC system will be made up of several modules. Each system is listed below with the information collected, maintained and/or shared.

The UC system collects multiple data elements to register and use the system to include user name, user ID, telephone number and email address. It syncs with Active Directory once daily. The system by default does not maintain or share PII. The system does not collect or store the information permanently. Data elements are collected temporarily through the utilization of Active Directory. The user name is stored in the database locally.

There are different modules of the UC system and these are as follows:

1) Cisco UC Manager (VoIP Telephone System)
2) Cisco Unity Connection (Voicemail)
3) Cisco Instant Messaging and Presence
4) Cisco WebEx Meeting Server
5) Cisco Prime Provisioning
6) Cisco Prime Assurance and Analytics

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

Yes

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

Name

Phone Numbers

User ID

Voicemails

Call Detail Records

Instant Messages

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?

10,000-49,999

For what primary purpose is the PII used?

This system will be integrated with Active Directory (AD) for user synchronization and single sign-on purposes. The AD is the system utilized by HHS as a directory service that Microsoft developed for Windows domain networks and is included in the HHS Windows Server operating systems. This system synchronizes users name, user ID, telephone number and email address and will be used for contacts information.

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

Not Applicable. There is no intent to utilize call data for secondary uses.

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

42 US Code, The Public Health and Welfare. This is the Title of the US Code that implements HHS and provides it with the legal authority to operate.

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

Government Sources

Within OpDiv

Other HHS OpDiv

Non-Governmental Sources

Identify the OMB information collection approval number and expiration date

The system does not collect information from members of the public.

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.

Not Applicable - This is an internal phone system in which information is synchronized with Active Directory.

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 utilize this system, minimal information needs to be synchronized with Active Directory and the user cannot opt-out to be part of this system. The information is needed to identify the correct person in Active Directory.

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

Uses and disclosures, and any other changes affecting individuals' rights or interests, are not expected to change. If it were, notification could be made through the system; using the contact information provided; through public notices; through supervisors or administrators; etc.

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.

Individuals can contact the Unified Communications Support group via email or phone.

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 system will sync with Active Directory daily to ensure the data's integrity, availability, accuracy and relevancy.

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

Users:

To sign in; for contact information

Administrators:

Update user account info if users have problems / issues with the system.

Contractors:

Some contractors may have administrative rights if they are in that support role, see 'administrator' rationale above.

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

Administrators are controlled and assigned rights through Terminal Access Controller Access-Control System (TACACS) and this will be used to provide access to the self-service portal. A two factor authentication will also be used. Customers will have the ability to reset their own pins. All administrative staff will sign and comply with the system administrator rules of behavior to ensure HHS operational policies are followed regarding administrator privileges and technical-use for systems. In the event that a PII incident is reported, the administrator has the ability to remove the PII from the system.

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 PII (name, e-mail address, and phone number) that is accessed is minimal information needed for the unified communications services. Most users of the system will therefore have access to all PII, but this PII is only minimally sensitive and will be used only accordance with HHS PII policy. All administrative staff will sign and comply with the system administrator rules of behavior to ensure HHS operational policies are followed regarding administrator privileges and technical-use for systems.

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.

As HHS employees, all personnel follow the HHS Office of the Secretary mandate that requires all system users (employees and contractors) to be exposed to security awareness materials, at least annually and prior to the employee's use of, or access to, information systems. This includes: Information Systems Security Awareness and Privacy Awareness Training. As part of the project training, employees are made aware of these regulations and trained in these policies.

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

Per HHS policy, personnel are exposed to security awareness materials, at least annually and prior to the employee's use of, or access to, information systems through online PowerPoint presentations and/or hard-copy PDF training. In addition, project team members will also be trained on the features and functionalities of the UC system. The frequency of this training will be initially at the start of project on-boarding, one-on-one in person training as well as online training on an as-needed basis.

Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?

No

Describe the process and guidelines in place with regard to the retention and destruction of PII.

The data elements and the corresponding General Records Schedule (GRS) are as follows:
Voicemail messages and instant messages, GRS 24, item 10;
Information about each call, time, duration, calling party and party called, as well as technical call quality elements, meeting IDs and PINs (exclusively configured by end users to access hosted meetings), GRS 12, item 4;
Active Directory information (user name, user ID, telephone number and e-mail address): GRS 24, item 6 (if audit able/investigative) or GRS 20, item 1c (if routine).

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

There is no PII pulled and retained in the system. However, the system uses Terminal Access Controller Access-Control System (TACACS) for purposes for administrative controls. Only authorized administrators have access to the system. The physical servers are hosted in an authorized data center in a government controlled area.