US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

07/14/2016

OPDIV:

OS

Name:

Hosted Unified Communications

PIA Unique Identifier:

P-8979424-114434

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.

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 Hosted Unified Communications (UC-H) system provides hosted and managed services for unified communications, contact centers and data networking. UC-H offers Unified Communications as a Service (UCaaS) by positioning a session-based experience, including voice, video, chat, presence, conferencing, messaging, contextual collaboration, federation, and rich client experiences on Bring Your Own Device (BYOD). The UC-H Hosted solution consists of the following core applications: Session Manager (SM), Communication Manager (CM) - Voice and Video Services, Application Enablement Services (AES), Presence Services, Session Border Controller (SBC), Messaging, Conferencing. Some elements of the UC-H offering include key elements in the service delivery, management, and monitoring tools. These tools include: IP Telephony Manager (performance metrics) and Client Enablement Services (CES) (mobility applications).

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

Voice mail can be saved and stored on the system if the users choose the option. User names, work emails, and work phone numbers, and work addresses are stored. Work email is sometimes used to contact users to let them know about the status of existing trouble tickets. Work addresses are used to specify location and placements of handsets/equipment. Only voice mail is stored and is purged after seven days.

Please Note:
--The HHS solution does not have instant message feature which is available via the Presence Services application.
--User-name and Password are stored in the active directory.
--There are two types of information on the users. First, their mailbox info includes their name and telephone numbers. That information is stored in an encrypted index International Business Machines ((IBM) Database2) and cannot be accessed without a valid set of credentials. The second type is contained in the information in any messages on the system which has three levels of security.
--Contractors, depending on their roles and privilege level have access to Personally Identifiable Information (PII) for phone operations and maintenance purposes. The PII stored and maintained on the system include, user name, password, phone number, e mail address, location information, voice message.

- For voice mail, message filenames are "randomly" assigned and stored in a distributed fashion across the file storage.
- Someone with access to the hard drive would not be able to tell which message is for which user just from the filename or location.

- The only way to associate an audio file on the file storage with a particular mailbox user would be if the person also had:

(a) access to the database and the login credentials for the actual database user account (this is known only to the installers, such as Applied Voice and Speech Technology (AVST) Field Engineer).

(b) knowledge of the AVST table structure and where to look for a message filename, and how to associate that filename to a mailbox (which is also obfuscated via the use of an internal ID for the mailbox, as opposed to simply associating it via the user's mailbox number).

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

Unified Communications-Hosted (UC-H) is a family of hosted and managed services for unified communications, contact centers and data networking. UC-H offers Unified Communications as a Service (UCaaS) by positioning a session-based experience, including voice, video, chat, presence, conferencing, messaging, contextual collaboration, federation, and rich client experiences on personal mobile devices.

The system collects/stores names, phone numbers, e-mail address, location Information, and will store voice mail from users if they so choose the option. User names (first and last names) and phone numbers are used to control system access. User names and phone numbers are contained in a searchable address book which all users have access to. The contact list is stored within UC-H and not directly on the phones. The users or HHS employees who created the voice messages are the only individuals who have access. Developers, administrators access the system with a user name and password that is access via Active Directory (AD), Radius. These credentials are not stored directly on the system, user names and passwords are stored in the AD. Contractors are not direct contractors since they do not use HHS email address as their official e-mail address nor work directly for HHS.

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

Yes

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

Name

Biometric Identifiers

E-Mail Address

Mailing Address

Phone Numbers

Voice Message

Password

User name

Location information

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?

500-4,999

For what primary purpose is the PII used?

The primary purpose for the PII is to access the system and for address booking. User names and phone numbers are available as a part of an organization wide address book which is available internally to all users.

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

N/A. No 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?

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.

09-90-0001 Tele. Directory / Locator System

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Email

Government Sources

Within OpDiv

Non-Governmental Sources

Private Sector

Identify the OMB information collection approval number and expiration date

This item is N/A. The system does not collect information from members of the public.

Is the PII shared with other organizations?

Yes

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

Private Sector

The PII is maintained using Siebel software and only authorized personnel with access privilege have access to the software for maintenance purpose only.

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

The sharing or disclosure of PII in the system is not subject to any agreements because there is no sharing or disclosure of PII information on the UC-H system.

Describe the procedures for accounting for disclosures.

The owner (contractor) of the system, UC-H, does not disclose PII with any individual nor entities. Only the authorized staff that works on Siebel software where PII is stored have access to Siebel and the system document the date, time and purpose, anytime they sign into the software for maintenance purposes.

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

Users consent by providing their information to be processed to obtain system access. A signed approval is received from the Operating Division (OPDIV) of HHS to add a new users to phone system list and the new users are informed about how the system works including nature of information that the system collect such as voice message. Notice is provided via email stating that the information provided will be processed in order to access the system.

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.

New user information is supplied on the Move Add Change or Delete (MACD) form by OPDIV for HHS. And if the user decides to opt out , the employee will inform the appropriate personnel at HHS and a new MACD form will be completed and send to the contracting company to remove the user from the phone system list.

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

HHS sends requests to add new names and work numbers via a MACD form that is sent through email. When major changes are implemented users are notified via email.

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.

Trouble tickets are created and resolved by contacting that individual user via work phone or work email for resolution. The Incident response team investigates the source and nature of the PII leak and communicates with the System owner as well as the concerned individuals on the findings.

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

Audit procedures are in place which includes randomly reviewing activity logs at least once annually with the intent to validate data integrity; identify, report any unauthorized activity. Audit records are captured by various components of the UC-H system. Associated issues are reviewed and resolved.

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

Users:

Gain system access.

Administrators:

System maintenance, issue resolution, account creation, review of security

Developers:

System testing, system upgrades.

Contractors:

HHS users including contractors will need to gain system access for agency related communication.

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

Strict role-based access control is enforced through security group membership that places limits on the authority of each user account.

Role-based access controls has been designed to provide separation of duties between user, administrator, and security auditor functions.

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.

Work phone numbers and associated names for this communications system is inherent. HHS UC-H users are listed in the system address book. Duties performed by employees are reviewed every sixty (60) days to ensure separation of duties and verify that users only have the system privileges that are necessary to complete their assigned tasks.

Strict role-based access control is enforced through security group membership that places limits on the authority of each user account. Role-based access controls have been designed to provide separation of duties between user, administrator, and security auditor functions. Detail of the Separation of Duties for Windows accounts is documented in the UC-H Standard Operating Procedure Manual.

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.

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 get trained on 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 on-line Power-point presentations and/or hard-copy PDF training. In addition, project team members will also be trained on the features and functionalities of the 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 on-line training on as-needed basis.

HHS users are trained on the features and functionalities of the system. The frequency of this training will be initially at the start of project on-boarding, and on 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 Information Technology Infrastructure & Operations (ITIO) is working with the Records Management Office to determine the appropriate record retention schedule. And the PII (with the exception of voice mail) will be maintained until a determination is provided.

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

Only system administrators can log into the system. UC-H is also protected by the network boundary. Also UC-H is protected by both physical and logical security. For the physical security, only authorized personnel with appropriate clearance are allowed into the data center. For the logical protection, the traffic on the system is monitored by Palo alto firewalls, Session border controllers and load balancers.