US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

06/22/2017

OPDIV:

HRSA

Name:

General Support Systems

PIA Unique Identifier:
P-9613167-017793

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?
Yes

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.
The Office of Information Technology (OIT) General Support System (GSS) is comprised of two operational data center locations which provide Disaster Recovery (DR) capabilities for the GSS. With respect to PIA, the data centers still operate logically as a single entity.

Describe the purpose of the system.
The OIT GSS is composed of systems and devices such as servers, firewalls, workstations, operating system software, data, and network infrastructure components. The purpose of the OITGSS is to provide computing and network services that support HRSA’s mission to improve the nation's health by assuring equal access to comprehensive, culturally competent, quality health care.

Describe the type of information the system will collect, maintain (store), or share.
PII collected from users/system administrators in order to access the system, consists of user credentials (i.e. username, password, Personal Identity Verification (PIV) card and/or email address).Users/system administrators include HRSA employees and direct contractors.

The system also contains e-mail messages, including any attachments, and documents uploaded to shared drives may include almost any type of HRSA information. However, users are not permitted to store SSNs in these share drives.

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

The OIT GSS is the underlying system and architecture which support HRSA, its mission and applications. The system collects user credentials from system users in order to control access to the system. The system also collects a user's contact information, such as name, phone number, and email address.

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

User Credentials

E-mail messages, including any attachments, and documents uploaded to shared drives may include almost any type of HRSA information.

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

Employees

How many individuals' PII is in the system?

500-4,999

For what primary purpose is the PII used?

PII is used for identifying HRSA employees. Credentials are used for accessing HRSA systems.

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

There is no secondary use for the PII in this system

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

In-Person

Email

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

Other OpDivs who have access to the HHS Global Directory

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

Not Applicable

Describe the procedures for accounting for disclosures.

Not Applicable

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 of the HRSA General Support System must acknowledge a HRSA approved system-use notification banner before access is granted to the system in accordance with the HRSA Information Security Policy and Procedure Handbook. Users are notified that they are accessing U.S. Government systems, and must consent to monitoring and recording of their activities, and any unauthorized use is prohibited and subject to penalty.

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.

Individuals do not have the option to not provide their contact information or user credentials. Credentials are required to access the system, and contact information is required to maintain contact with colleagues to accomplish the agency's mission.

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

Users do not have the ability to consent to their information being collected. Credentials are required to access the system. Contact information is required for users to be contacted in order to carry our HRSA's mission.

When users must change their credentials, they receive notification that they must change their password.

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.

The PII is collected directly from the user. If the user has a concern they may bring of the concern with the HRSA authorized official that is collecting the information from the user.

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

When a user leaves HRSA and no longer needs a user account, a help desk ticket is put in to remove the user after approval from a manager. The administrator removes the user account and all related PII data.

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

Users:

Users will have access to other user's e-mail addresses and names in order to contact them for work related purposes.

Administrators:

To make changes to the system

Contractors:

Contractors who are users will also have access to user's e-mail addresses and names in order to contact them for work related purposes.

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

All users may access user's email addresses and names in order to contact them for work related purposes.

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.

Users only have access to names, e-mail addresses and phone numbers, which is essential to make contact with other users in order to perform job duties. Users do not have access to other user's credentials.

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 Department users to include federal employees, contractors, and other system users must take the HRSA Security and Privacy Awareness Training. Users must also review and sign an acknowledgement statement of the HHS Rules of Behavior (RoB). This acknowledgment must be completed before users receive access to the system, and annually thereafter.

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

System users who have significant roles and responsibilities that could potentially impact the security posture of the system receive the HRSA significant user training.

Executives receive the Executive user 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.

Once a user leaves HRSA, their account is deleted, along with their email address. Their credentials do not need to be retained.

Disposition Authority: DAA-GRS-2013-006-003 (GRS 3.2, Item 30). System not requiring special accountability for access. Temporary. Destroy when business use ceases.

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

Security controls for this system include redundant Cisco firewalls; redundant intrusion monitoring systems including Securify and Proventia; 24x7 monitoring of the perimeter defenses; antivirus systems with automatic updates for both workstations and servers from McAfee and Symantec; Ad-aware anti-spyware software; and routine certification and verification activities. Access is limited to those requiring access to the system and is protected by username/password controls with enforced complexity requirements. Physical controls include card reader access to authorized individuals and cameras for monitoring and recording Data Center activity.

Identify the publicly-available URL:

https://www.hrsa.gov

Does the website have a posted privacy notice?

Yes

Is the privacy policy available in a machine-readable format?

Yes

Does the website use web measurement and customization technology?

Yes

Select the type of website measurement and customization technologies is in use and if it is used to collect PII.

Session Cookies that collect PII.

Does the website have any information or pages directed at children under the age of thirteen?

No

Does the website contain links to non- federal government websites external to HHS?

No

Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?

Yes