

# US Department of Health and Human Services

## Privacy Impact Assessment

**Date Signed:**

04/25/2016

**OPDIV:**

OS

**Name:**

Managed Application Hosting Center

**PIA Unique Identifier:**

P-5704136-908140

**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)?**

No

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

PIA Validation

May include any PII that an underlying application creates. HHS's applications range in purpose from financial management systems to emergency response systems.

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

Not applicable.

**Describe the purpose of the system.**

The Managed Application Hosting Center (MAHC) General Support Center (GSS) was established to maintain a secure data center for hosting multiple HHS applications.

MAHC may include any Personally Identifiable Information (PII) that an underlying application creates. HHS' applications range in purpose from financial management systems to emergency response systems. Each application/system hosted by MAHC has a Privacy Impact Assessment (PIA).

MAHC GSS administrators do not have access to the HHS application backup data stored within the GSS. MAHC personnel only assist with restoring this data to the application servers and database at the request of the application owner.

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

The MAHC GSS collects and stores data for backup purposes only for the applications that it hosts. It does not disseminate information. MAHC may contain any and all data that the hosted applications create. MAHC uses the information only for the purposes of backing up the data. Underlying systems use the data for a broad range of purposes, reflected in those systems' PIAs.

Other data stored is related to data log files and management data regarding the performance of that application. All HHS/Office of the Secretary (OS) Staff Divisions (StaffDivs) supported by Program Support Center (PSC) can store data in some of the applications that are hosted in the MAHC.

User credentials are maintained for system administrators (OS employees and direct contractors) in MAHC.

Log Files and Management Data could contain the following:

Server User Access and Authentication Logs

Server Resource Utilization Logs including Central Processing Unit/Memory/Disk Read and Write  
Network events

Database user access and authentication logs

Permission Modification logs

User created/deleted logs

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

The MAHC GSS is a General Support System (GSS) that provides the protected environment through which HHS connects to its major applications. MAHC hosts 52 applications and each application is required to complete a separate PIA.

Data processed on the MAHC GSS is considered Sensitive But Unclassified (SBU). Classified information is not permitted on the system.

Other data stored is related to data log files and management data regarding the performance of that application. All HHS/OS StaffDivs supported by PSC can store data in some of the applications that are hosted in the MAHC.

User credentials are maintained for system administrators (OS employees and direct contractors) in MAHC.

Log Files and Management Data could contain the following:

Server User Access and Authentication Logs

Server Resource Utilization Logs including Central Processing Unit/Memory/Disk Read and Write  
Network events

Database user access and authentication logs

Permission Modification logs

User created/deleted logs

**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

May include any PII that an underlying application creates. HHS' applications range in purpose from

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

Employees

**How many individuals' PII is in the system?**

100-499

**For what primary purpose is the PII used?**

Login credentials (email address and password) are collected to support and administer MAHC. To access the system, administrators enter login credentials.

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

Secondary use of PII is addressed in the PIAs for each of the applications hosted on MAHC.

**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.**

Online

**Government Sources**

Within OpDiv

**Identify the OMB information collection approval number and expiration date**

Not applicable.

**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.**

Consent for data collection and use depends on the underlying business processes of each application. Consent is not collected for system and data backup purposes in and of itself, but as part of consent for the underlying activities.

The collection OS employee and direct contractor user credentials being saved by MAHC is inherent to employment. Individuals requesting access to MAHC must sign an account request form. Prior to granting access, review and approval is required by the main MAHC System Information System Security Officer (ISSO).

**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.**

Consent for data collection and use depends on the underlying business processes of each application. Consent is not collected for system and data backup purposes in and of itself, but as part of consent for the underlying activities.

An option for users to opt-out of having their login credentials stored within the MAHC system is not available because it is fundamental to the function of the system. Potential user cannot 'opt-out' of providing his or her PII. The PII is needed to create a user account in order to access the MAHC system.

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

Only OS employees and direct contractors credentials are accessed/stored by the system. The expectation of user credentials being saved by OS systems is inherent to system access. Individual requesting access to MAHC must sign an account request form. Prior to granting access, review and approval is required by the MAHC system owner.

Major changes to the system that affect individuals' rights or interests are not expected. If these were to occur, individuals would need to be informed through the business processes underlying the individual applications stored on the MAHC.

This is the responsibility of the business process owner or system owner for the individuals systems that GSS contains and backs up.

**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.**

1. Users and system administrators provide notification of PII events at HHS by contacting the Office of Information Technology Infrastructure and Operations (ITIO) Service Desk to report the incident.
2. The ITIO Service Desk routes PII incidents to the HHS Computer Security Incident Response Center (CSIRC).
3. The CSIRC notifies the HHS Privacy Incident Response Team (PIRT), Information Systems Security Officer (ISSO) for the related system then supports investigation and mitigation of the privacy incident.
4. The PIRT executes investigation, mitigation and any notification related to the privacy incident.

If the user credential information is inaccurate such that a name is misspelled or an e-mail is incorrect, then a simple e-mail to the OS Access Authority with the details of the change would be sufficient to correct the problem and amend the record within MAHC.

**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 user credential information is initially entered into MAHC via a request form, to allow access to the system. The form must be approved by the employee's manager and Contracting Officer Representative. The MAHC system automatically requires users to review their access information annually and confirm that it is accurate. Further, when an employee or direct contractor is terminated, their access to MAHC is terminated and their MAHC information is deleted.

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

**Administrators:**

Administrators of the MAHC system may be direct contractors or OS employees and will be able to generate a list of local system administrators by login User ID. This is necessary to perform their job as administrators of applications or local systems and have the ability to add, edit or delete user IDs. The only information that is accessible is the User name/User ID.

**Contractors:**

Local Administrators of the MAHC system, may be direct contractors or OS employees and they may have access to a list of local system administrators by login User ID. This is necessary to perform their job as administrators of MAHC.

**Others:**

All use and access of PII occurs at the level of the underlying applications. Use and access is addressed in the PIAs of those individual systems.

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

MAHC GSS administrators do not have access to the HHS application backup data stored within the GSS. MAHC personnel only assist with restoring this data to the application servers and database at the request of the application owner.

Prospective users must sign an account request form. The account request form must also be filled indicating the minimal access required to perform one's tasks. Prior to granting access, review and approval is required by the system owner.

**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.**

MAHC GSS administrators do not have access to the HHS application backup data stored within the GSS. MAHC personnel only assist with restoring this data to the application servers and database at the request of the application owner.

System Administrators review user accounts at least annually. Any anomalies are addressed and resolved by contacting the user, and modifying their user data, or by removing their access if no longer required. Activities of all users including system administrators are logged and reviewed by the MAHC system ISSO to identify abnormal activities if any.

**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 Privacy Awareness and Security Awareness Training

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

N/A

**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.**

The MAHC follows HHS guidelines for backup data retention and destruction. Depending on the Service Level Agreement for each application, daily backups are stored on-site for up to thirty (30) days, weekly backups are stored off-site for thirty (30) days and longer. Per request from application owners, Program Support Center Property Management needs to pick up media from the MAHC and take it to their facility to be wiped. This allows verification and accountability that the media has been wiped per HHS guidelines.

User Credentials retention schedule: General Records Schedule (GRS) 3.2. Item 010, Disposition Authority: DAA-GRS-2013-0006-0001. Destroy 1 year(s) after system is superseded by a new iteration or when no longer needed for agency/IT administrative purposes to ensure a continuity of security controls throughout the life of the system."

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

The MAHC only stores PII for backup purposes. The backup system is stored behind a firewall from all other networks. Access to the management network is restricted to select personnel. All backups and restorations are performed by the operations team to ensure appropriate data is backed up and restored. Off-site archival is encrypted.

Controls are as follows:

**Administrative Controls:** Include controls which require action on part of human resources.

Administrative controls are the process of developing and ensuring compliance with policy and procedures. They tend to be things that employees may do, or must always do, or cannot do. The administrative controls include, but is not limited to, incident handling, controlled maintenance, and access control for transmission medium.

**Technical Controls:** Include a class of controls in security that are carried out or managed by computer systems. The technical controls include, but is not limited to, continuous monitoring, information system back-up, and telecommunication services, and maintenance tools.

**Physical Controls:** Include controls implemented to protect systems, buildings, and related supporting infrastructure against threats associated with their physical environment. The physical facility is usually the building, other structure, or vehicle housing the system and network components. The physical controls include, but is not limited to, media storage, physical access and authorization, and boundary protection.