US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

12/06/2024

OPDIV:

ACF

Name:

Peer Monitoring Database Management System

PIA Unique Identifier:

P-5023415-855517

The subject of this PIA is which of the following?

Minor Application (stand-alone)

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.

Contractor

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.

No changes were made.

Describe the purpose of the system.

The Peer Monitor Data Management System (PMDMS) is a workflow and routing application designed for internal use to manage and track Federal Project Officers' (FPO) travel plans, retain site visit information, and to provide a method for the Family & Youth Services Bureau (FYSB) to generate biennial reports to Congress regarding various site visits to the grantees supporting the FYSB programs.

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

The information contained within the system collects names and contact information of the Peer Monitors: The Personally Identifiable Information (PII) data that are contained within the PMDMS

are: Data Universal Numbering System numbers (DUNS numbers), grant numbers, grant duration, address, phone number, grantee contact's phone and e-mail address, and assigned Federal Project Officer's phone numbers. Also, the PMDMS uses 2-Factor Authentication that includes login credentials (username and password) and an authentication code sent to a user's email address. The PMDMS collects the login credentials (username and password) for the Peer Monitors, Federal Project Officers, Central Officers and Admin Roles. The PMDMS application stores grantee information using a copy of the data from the Grants Solutions database, schedules onsite reviews to the grantee sites, the dates of the visits, dates of travel, who authorized the visit, notes from the visit, and outlines if the visit was successfully executed post site visit.

The PMDMS also stores information regarding site visits approved by Regional Program Managers for the Federal Project Officers to complete, with or without a Peer Monitor, and provides an after-action report.

The PMDMS receives grantee name, address, and DUNS # (The D-U-N-S Number is used around the world to identify and access information on businesses. A D-U-N-S Number identifies a company's Dun & Bradstreet business credit file, which may include firm geographic data [company name, address, phone number, etc.], corporate family relationships [headquarters, branches, subsidiaries, etc.], and scores and ratings that assess different financial health indicators. Taken all together, this profile of information is called the Dun & Bradstreet Live Business Identity. Potential partners and lenders can request a business credit report about your business using your D-U-N-S Number or other business identifiers.) from Gant Solutions in an excel spreadsheet, that then gets uploaded into the PMDMS database.

For login accounts to the PMDMS, a users' First Name, Last Name, and E-mail address are the required data.

NOTE: The term information pertains to a DUNS number, grant numbers, grant duration, address, phone number, grantee contact's phone and e-mail address, assigned Federal Project Officer's phone, and e-mail address.

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

The PMDMS simply stores information regarding site visits approved by Regional Program Managers for the Federal Project Officers to complete, with or without a Peer Monitor, and provide an after-action report. The information collected is maintained and stored within the Amazon Web Services (AWS) Cloud. All information stored in the PMDMS will be kept indefinitely until a formal records schedule is approved by the National Archives and Records Administration (NARA) with the exception of system access records, which are maintained temporarily in accordance with the NARA general records schedule (GRS).

The information includes: users' First Name, Last Name, and E-mail address; DUNS number, grant numbers, grant duration, address, phone number, grantee contact's phone and e-mail address, assigned Federal Project Officer's phone and e-mail address, and login credentials (username and password).

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

Mailing Address
Phone Numbers
User Credentials
DUNS Number
Grant Numbers; Grant Duration

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

Employees
Business Partner/Contacts (Federal/state/local agencies)
Vendor/Suppliers/Contractors
Peer Monitors are assigned by the Federal Project Officers. The Peer Monitors perform the site visits only. They do not have badges. Peer Monitors are individuals who work at a Runaway and Homeless Youth (RHY) grantee site and are hired by Gray Matters Technology Services (GMTS), at the recommendation of FYSB, to perform onsite monitoring of RHY grantees.

How many individuals' PII is in the system?

<100

For what primary purpose is the PII used?

The primary purpose for the collection and maintenance of PII within the PMDMS includes user account management and Peer Monitor correspondence.

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

N/A

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

5 USC 301 Departmental regulations.

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.

09-80-0341 FYSB Research and Evaluation Project Records.

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains
Email
Other
Government Sources
Within OpDiv
Other
Non-Governmental Sources
Public
Other

Identify the OMB information collection approval number and expiration date

N/A

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.

When the direct contractor from Gray Matters Technology Services (GMTS) is notified by FYSB of a new PMDMS user, the admin sends an e-mail to the new user with his/her username and temporary password. The user is then instructed to change his/her password to ensure privacy.

The Project Manager creates the account as the Account Administrator and sets up the Peer Monitor User ID and Password only. The Peer Monitor then logs into the system, chooses a password, and registers. All users of the system are made aware that personal information is collected as part of the user account registration process. However, the language included in the e-mail that is sent to each new user during the account creation process is being modified to include language informing the user that the system will be collecting PII during the account creation process. A revised e-mail was (implemented on 8/15/2019) sent to each user during account creation. The plan is to retroactively notify current users of the system update via e-mail.

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.

Any user who wishes to opt-out will not be granted a system account; however, this may not be an option if the user’s job duties require access to the system.

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

All users of the system are notified of any system updates or maintenance requirements through email notification.

An e-mail is sent to users over a weekend, typically for any systems updates or maintenance requirements.

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 which have their PII in the PMDMS are directed to email the Project Manager if they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate. The Project Manager can be reached via help@gmatterstech.com. The Project Manager will review the e-mail and forward it to the Information Technology (IT) Developer for action.

Additionally, FYSB has a responsibility to report any suspected or confirmed incidents involving the PMDMS to the ACF Incident Response team and a federal supervisor.

All incidents are reported first to the FYSB Contract Office Representative (FYSB COR) relating to the PMDMS, then sent to the ACF incident response team for any additional guidance that may be required.

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 insured through role-based access control which limits the number of users that

have privileged capabilities. Roles are separated by user type within the system.

Data Availability is handled by the systems' hosting infrastructure, AWS. The AWS GSS Service Level Agreement (SLA) guarantees 99% availability using multiple availability zones, a live synced database, and daily backups.

Data Accuracy is ensured through annually required user profile validations. At this time users are prompted to confirm their information is correct or to make changes as needed. Users are required to select a checkbox validating the information is correct before they can continue using the PMDMS.

Data Relevancy is maintained by following specific retention and destruction schedules.

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

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

The Family and Youth Services Bureau (FYSB) identifies which individuals are granted roles and permissions based on job assignment. The FYSB Contract Officer Representative (COR) will notify GMTS' Project Director of granting a role in PMDMS, who will in turn notify the PMDMS Admin. Upon notification, the Admin User sends a username and temporary password to the new PMDMS user.

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.

Access to the system is determined by user-defined roles. The roles determine what a user will see within the system. The system enforces the access controls defined by the users' roles.

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.

PMDMS users are presented an electronic copy of the Rules of Behavior (RoB) for Use of HHS Information Resources (HHS RoB). Users must read the HHS RoB and sign the accompanying acknowledgement form. The contractor maintains a file of all signed acknowledgement forms for PMDMS users. The process is repeated annually, and only users with a signed HHS RoB acknowledgement form on file shall retain access to the PMDMS. This process will be implemented as of October 1, 2019, for existing PMDMS users.

Personnel (e.g., Central Officers, Regional Program Managers, Federal Project Officers, Peer Monitors, and/or Grantee Users) undergo annual Cyber-Security Awareness Training. The contractor maintains a tracking spreadsheet that identifies the trainings, forms of acknowledgement, and authorizations applicable to personnel and PMDMS users. The tracking sheet is updated at least annually or when applicable actions take place for new or current users.

Users are subject to the standard Cyber-Security Awareness Training, as well as being subject to

the Rules of Behavior for Use of HHS Information Resources as part of HHS's Security Awareness Training Policy. Threat and security awareness training is conducted in October of each calendar year.

Training is conducted for PMDMS users (Central Officers, Regional Program Managers, Federal Project Officers, Peer Monitors, and Grantee Users) only and Refresher training can be requested from the COR. Training is scheduled and held via webinar.

Additionally, all personnel including both direct contractors and government personnel are required to participate in the ACF annual security compliance training and privacy training.

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

PMDMS trainings are held quarterly via GoToWebinar for all Federal Project Officers and Peer Monitors – these sessions are conducted separately as the FPO interface is different from the Peer Monitor interface. GMTS offers the following PMDMS trainings:

- PMDMS Overview (login, grantee search, home page interface, etc.)
- Understanding Logistics Support Requests (LSRs)
- Monthly Contact Forms and Process
- Onsite Monitoring Instrument (OMI) Online Form and Process
- OMI PDF Completion
- 360 Feedback Forms and Process

During each training, FPOs and Peer Monitors can ask questions during the live training and receive immediate feedback from the trainers.

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 PMDMS retention schedule is under National Archives and Records Administration (NARA) review.

The system user account records should follow NARA GRS 3.2 Item 030.

Item 030 System access records: Destroy five years after system is superseded by a new iteration, is terminated, defunded, or no longer needed for Agency/IT administrative purposes.

Longer retention is authorized if required for business use.

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

The application is hosted within Amazon Cloud AWS platform
Administration Control. Individuals that obtain access to the system must be approved by Regional Program Managers. Access to the system is based on user-defined roles and granted based on the principle of least privilege. Application user manual and user training are used to inform how to secure and handle PII.

Technical Controls: The application requires user/password authentication. All interaction within the web application is encrypted with Secure Sockets Layer (SSL) encryption. All user passwords are encrypted before storing within the database. The database that stores the PII data is not publicly accessible. The database server access is controlled by an AWS security group allowing only inbound IPs that have been whitelisted permission to Remote Desktop Protocol (RDP) into the server. The server is further secured by Window account authentication to login accounts.

Physical Controls: AWS data centers are selected to mitigate environmental risks, such as flooding, extreme weather, and seismic activity. AWS has built in redundancy so in the event of a failure, automated processes move traffic away from the affected area. Core applications are deployed to an N+1 standard so that in the event of a data center failure, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites. Within AWS, critical system components are backed up across multiple, isolated locations known as Availability Zones. Each Availability Zone is engineered to operate independently with high reliability. AWS provides physical data center access only to approved employees. All employees who need data center access must first apply for access and provide a valid business justification. These requests are granted based on the principle of least privilege, where requests must specify to which layer of the data center the individual needs access and are time-bound.

Identify the publicly-available URL:

https://fysbdms.acf.hhs.gov

Note: web address is a hyperlink.

Does the website have a posted privacy notice?

No

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.

Does the website have any information or pages directed at children uner 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?

null