US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

09/20/2017

OPDIV:

OS

Name:

Payment Management System

PIA Unique Identifier:

P-4771987-154848

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?

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.

Upgraded the Hardware from HP servers to Solaris as part of a Payment Management System (PMS) Modernization effort. Encrypted live data. Increased the network speeds of PMS data transmission.

Describe the purpose of the system.

The PMS is a web based system that electronically transmits Federal grant funds to grantees via the Federal Reserve Bank (FRB). The PMS accountants transmit grantee payment requests via authorized FRB virtual private network (VPN) access maintained by the FRB. PMS provides real time accounting information to grantees and Federal agencies.

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

The PMS maintains automated interfaces with grant awarding agencies.

The information the agency collects, maintains, or disseminates is an HHS standard financial record, which is exchanged to identify new grants and modification to existing grants. The PMS provides output to agencies with regard to disbursement data, synchronization data, standard form (SF) SF-224 data (STATEMENT OF TRANSACTIONS (Financial Management Service (FMS) 224) Reporting by Agencies for which The Treasury Dept. disburses), and daily payment information to agencies that request it.

The information contains PII in the form of Social Security Number (SSN), bank and routing data, Internal Revenue Service (IRS) data (Employer Identification Number), Personal Names, mailing address, taxpayer ID, Personal Phone Numbers, and Personal Email Addresses. Grantee information is collected via a Standard Form (SF) 1199A, Direct Deposit form that is either mailed, faxed or emailed from the grant recipient to a Federal staff member that enters the information into the PMS. The PMS maintains PMS user information for access purposes. This information includes; user names, passwords and email addresses. PMS employees total encryption; data at rest, in transit and live.

Account Credentials are stored on the Access Management System (AMS) and the PMS application. PMS uses two factor authentication.

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

The PSC, through the Division of Payment Management (DPM), provides grant payment and cash management services to all HHS agencies and ten (10) major non-HHS agencies on a fee for service basis: Department of Health & Human Services(HHS); Department of Labor (DOL); Department of Agriculture (USDA); Department of the Treasury; Department of State (DOS); Department of Veteran's Affairs (VA); Department of Homeland Security (DHS); Executive Office of the President (EOP); United States Agency for International Development (USAID); National Aeronautics and Space Administration (NASA); Corporation for National and Community Service (CNCS); and Small Business Administration (SBA).

PMS is a full service centralized grants payment and cash management system, supporting over 31,000 Grant Recipient Accounts. PMS is the largest grants payment and cash management system in the federal government. The System is fully automated to receive payment requests, edit the payment for accuracy and content, transmit the payment to either the Federal Reserve Bank or the U.S. Treasury for deposit into the grantee's bank account, and record the payment transactions and corresponding disbursements to the appropriate account(s). PMS uses an automated end-user certification for the grantee community. This feature allows the system to confirm the identity of grantee recipients (including users that are not federal employees) when they use the system.

PMS operates for the purpose of providing a central system capable of paying most Federal assistance grants, block grants, and contracts. The main purpose of this system is to serve as the fiscal intermediary between awarding agencies and the recipients of grants and contracts, with particular emphasis on: Expediting the flow of cash between the federal government and recipients, recording award authorizations that are initiated by the grant awarding agencies; processing grant recipient requests for funds, transmitting recipient disbursement data back to the awarding agencies, and managing cash flow advances to grant recipients.

The information contains PII in the form of Social Security Number (SSN), bank and routing data, IRS data, Personal Names, mailing address, taxpayer ID, Personal Phone Numbers, and Personal Email Addresses. Grantee information is collected via a Standard Form (SF) 1199A, Direct Deposit form, that is either mailed, faxed or emailed from the grant recipient to a Federal staff member that enters the information into the PMS.

Login credentials are maintained by the HHS Access Management System (AMS). IT developers and IT infrastructure support of the Servers and Networks/Firewalls are provided by the National Institutes of Health (NIH) Federal Data Center.

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

Yes

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

Social Security Number

Name

E-Mail Address

Mailing Address

Phone Numbers

Financial Accounts Info

Taxpayer ID

Employer Identification Number

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

Employees

Business Partner/Contacts (Federal/state/local agencies)

How many individuals' PII is in the system?

10,000-49,999

For what primary purpose is the PII used?

The primary use of PII is disbursement of grant funding to authorized grantees, cash flow, and reporting. PII is also used to report disbursement data back to the financial system of record (US Federal Government Authorized Accounting Systems, i.e. United Financial Management System (UFMS)) for reconciliation purposes.

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

PII may be used if required by reporting requirements, to audit the grant funding process, or for the Operating Division (OpDiv) to review its activity and evaluate issues related to efficiency, budgeting, and operations. Data is never released without program authorization.

Describe the function of the SSN.

PMS operates for the purpose of providing a central system capable of paying most Federal assistance grants, block grants, and contracts. HHS is required to record these transactions and include the Taxpayer Identifier Number (TIN) associated with each payee. In a very limited number of instances PMS uses the SSN as the TIN when a grantee does not have a separate Employer Identification Number (EIN), as allowed under tax laws. PMS is a subledger to the financial system as such our primary attribute for PII is the TIN as a disbursing agent.

Cite the legal authority to use the SSN.

In a very limited number of instances PMS uses the Social Security Number (SSN) as the TIN when a grantee does not have a separate EIN, as allowed under tax laws, Executive Order (EO) 9397, “Numbering System for Federal Accounts Relating to Individual Persons,” November 22, 1943, which states in part that “[A]ny Federal department, establishment, or agency may, whenever the head thereof finds it advisable to establish a new system of permanent account numbers pertaining to individual persons, utilize the Social Security Act account numbers assigned pursuant to Title 26, section 402.502 of the 1940 Supplement to the Code of Federal Regulations and pursuant to paragraph 2 of this order.”

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

The implementation of this system, is authorized by 5 U.S.C. 301 and section 205(c) of the Federal Property and Administrative Services Act of 1949, as amended by 40 U.S.C. 486(c), as delegated by the Secretary. Budget and Accounting Act of 1950 (Pub. L. 81-784); Debt Collection Act of 1982 (Pub. L. 97-365); Debt Collection Improvement Act of 1996 (Pub. L. 104-134, sec. 31001.
More precise HHS acquisition rules are issued in the Code of Federal Regulations (CFR) at 48 CFR Chapter 3. OMB Circular No. A-102 addressing the administration of grants to state and local governments and federally-recognized Indian tribal governments; OBM Circular No. A-110 addressing the administration of grants to institutions of higher education, hospitals, and other non-profit organizations; OMB Circular No. A-123 addressing internal controls; and The Treasury Financial Manual (TFM) Volume I, Part 5, Chapter 1000 specifying responsibilities and liabilities of agencies with delegated disbursing authority.

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.

09-90-0024, Fin. Txns.of HHS Acctg & Fin. Offices; General Services Administration (GSA)/

GOVT 9, System for Award Management

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

Hardcopy

Email

Government Sources

Within OpDiv

Other HHS OpDiv

State/Local/Tribal Foreign

Other Federal Entities

Non-Governmental Sources

Private Sector

Identify the OMB information collection approval number and expiration date

Not Applicable. The Payment Management System is not a direct public facing system and does not collect PII information from the general public. The information used is in established agreements between the Granting Agencies and their Grantee population.

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.

Notification and consent is obtained by the completion of the Grant Application, which explicitly states the nature of the use of the PII.

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.

Notification and consent is obtained by the completion of the Grant Application (they have opted-in to the collection, hence no need to provide an opt-out), which explicitly states the nature of the use of the PII.

The Grant Application includes the electronic process whereby PII data is shared with awarding institutions, the Federal Reserve and other involved banking institutions. The Notice of Consent is in written format.

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

Users supply information voluntarily for the purposes of conducting business or otherwise receiving payments from HHS. Consent for this collection is implicit in the process. In the event any changes were made to the system that affected individuals' rights or interests, these individuals could be contacted using the PII they have provided. Conversely, a user that wished to learn more about the use of their PII may consult the PMS website, which directs users to the HHS Cybersecurity Team and/or the HHS Office of the Privacy Coordinator.

Initial requests for grants include disclosure to the grantee. We announce, via DPM Website, all uses of PII under mandates.

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.

Grantee may contact their Certifier or HHS directly by email or phone. The user achieves access to the PMS utilizing a web portal that is the PMS home page (https://pms.psc.gov/). At the bottom of the PMS home page, the user can click Privacy Policy, which takes them to the HHS.gov Privacy Policy Notice page (http://www.hhs.gov/Privacy.html) where there is a Notice and link in the first section of the page to go to the HHS.gov health Information Privacy page (http://www.hhs.gov/ocr/privacy/index.html). On the left pane of this page there is a link for How To File A Complaint (http://www.hhs.gov/ocr/privacy/hipaa/complaints/index.html)

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

Payments are made to grantees on an ongoing basis. The grantees have access to their accounts and can submit changes as they see fit. As this is the best source of obtaining this information we leave that review to the grantee as updates follow a standard practice.

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

Users:

Users only have access to their specific accounts.

Administrators:

System administrators whom provide system maintenance and operating system patching.

Developers:

The PMS development team whom provide system updates.

Contractors:

The PMS Help Desk facilitate the resetting of passwords.

Others:

The HHS Office of the Inspector General (OIG) conducts annual Audits.

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

Based on the sensitivity of the PII in PMS, security measures are employed in granting access to the system. Users are granted access to screens containing PII only if they have 1) need to use that information as part of their official duties, and; 2) have received a security level VI clearance or higher. This applies to contractors as well and is enforced by HHS security and privacy protection policies. PMS personnel must hold appropriate clearances that provide for *operations and maintenance (O&M) for the system. Grantees are provided access to their own information and do not have the ability to access other grantee information. PMS employees segregated access and least privileges for Granting Agency users, Grantees, PMS accountants (Federal staff) and PMS application developers (direct contractors) as well as PMS Help Desk personnel whom perform password resets and provide general PMS instructions to the Grantees.

Operations and Maintenance - When a mature system like the PMS is in a steady state of operation and is continuing to perform, a contract is issued to maintain the system, we call this an O&M contract. A replacement system would not be an O&M contract for example. Operations would mean daily or monthly security patching requires testing before implementation into the production environment. Maintenance means the day to day activities that a financial system requires to function for example, databases need to be maintained daily to ovoid corruption by adjusting table space.

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.

There are very limited number of instances where an SSN is entered in the system as the TIN. However, all DPM system users have access to all PII. For system developers, only those individuals who need access to databases to test the performance of the system have access to any database contents, but again, they have access to all PII. PMS access has segregated access and least privileges for Granting Agency users, Grantees, PMS accountants (Federal staff) and PMS application developers (direct contractors) non-direct contractors (PMS Help Desk) are used for Password resets and general PMS information.

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 users receive Department-level Privacy Awareness Training and Information System Security training.

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

High level users of the PMS complete privacy and security training specific to the National Institutes of Health.

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.

Records are purged from automated files once the accounting purpose has been served; printed copy and manual documents are retained and disposed of after 6.3 years in accordance with Government Accountability Office principles and standards as authorized by the National Archives and Records Administration. REF DAA-GRS-2013-0005

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

All PMS data, PMS databases and the PMS application are fully encrypted, i.e., data at rest, data in transit and live PMS application access.

All data collected to support the processes of the PMS is stored in tables. The information is secured through multiple levels of security and access controls have been established to authenticate the user and to determine if the user has the authorization to perform actions requested. The access controls are supplemented with a secure network at both National Institutes of Health (NIH) and PMS.

Administrative Controls:

Certification & Accreditation (C&A)

Approved System Security Plan(SSP) - Contingency Plan

Backups

Off-site Storage

User Manuals

Contractor Agreements

Least Privilege

PII Policy

Technical Controls:

User ID and Passwords

Firewall

Virtual Private Network

Intrusion Detection

Process for monitoring and responding to security incidents - Encryption

Common Access Cards (CAC)

Public key infrastructure (PKI)

Physical Controls:

Guards

ID Badges

Closed Circuit Television(CCTV)

Keycards

Kastle Keys, Coded keys that provides elevator floor access -Biometrics

Identify the publicly-available URL:

https://pms.psc.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.

Web Beacons that do not collect PII.

Web Bugs that do not collect PII.

Session Cookies that do not collect PII.

Persistent Cookies that do not collect PII.

Other technologies that do not collect PII:

N/A

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