

US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

05/24/2016

OPDIV:

OS

Name:

Integrated Time and Attendance System

PIA Unique Identifier:

P-7427215-154848

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?

No

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

Significant System Management Change

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

Integrated Time and Attendance System (ITAS) was integrated with Access Management System (AMS) simplified sign on solution allowing ITAS users to use AMS as the gateway to ITAS. Use of AMS is recent and constitutes a "major change" (significant merging) as of September 4, 2012.

Describe the purpose of the system.

ITAS is a timekeeping-by-exception application that supports most aspects of tracking and reporting work hours and leave for HHS employees. Exception is in that timecards are automatically generated each pay period for eligible employees.

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

The system Collects employee names, employee identification numbers (Social Security numbers (SSN) and Access Management System at HHS (AMS/HHS) identification numbers), hours worked, vacation leave hours earned and used, and sick leave hours earned and used. However, PII, such as SSN and name, are manually transferred by the timekeeper from the Enterprise Human Resource Payroll System (EHRP) into ITAS.

User credentials are stored in AMS for accessing ITAS.

PII is used as indicated.

Submission of this information is required to permit payroll processing for employees.

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

ITAS is a timekeeping by exception application that supports most aspects of tracking and reporting work hours and leave for federal employees. ITAS provides users with access to real-time leave balances and ensures that users accurately record work activity by enforcing time and attendance policies and procedures specific to the Federal Government. ITAS contains rules specific to data entered by Employees, Timekeepers, Approving Officials, Administrative Officers, and ITAS Administrators. In addition to Employee PII, hours worked, vacation leave hours earned and used, and sick leave hours earned and used are collected and stored.

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

Military Status

Employment Status

Employee ID numbers (SSN and HHS ID), hours worked, vacation leave hours earned and used,

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

Employees

No

How many individuals' PII is in the system?

10,000-49,999

For what primary purpose is the PII used?

The information entered into this data system becomes a part of the accelerated time and attendance data collected and documents daily time and attendance for employees. The primary use of the information is to prepare time and attendance transactions as input to the Defense Finance and Accounting Service (DFAS), the system HHS uses to track information needed throughout the payroll cycle and to eventually compute paychecks.

The ITAS data is secured-file transfer protocol (FTP) over to our mainframe system, hosted by the National Institutes of Health (NIH) Center for Information Technology (CIT_ Data Center where it is processed with other HHS Operating Divisions (OpDivs) time and attendance data. That data is then shared with the Department's payroll provider Defense Finance and Accounting System. The purpose of sharing the information is to provide data to DFAS for payroll processing. User information is also shared with the AMS system for the purposes of facilitating single sign-on (SSO).

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

None

Describe the function of the SSN.

The SSN is used to send transactions to DFAS which uses the SSN as the primary detail record to post the transactions to the employees record and not employee identification.

Cite the legal authority to use the SSN.

E.O. 9397 and 31 U.S.C. 7701(c) (2) authorize the collection of the SSN. The former is the Executive Order noting that the SSN is to be used for various official government purposes, including as the Taxpayer Identification Number (TIN), and the latter states "The head of each Federal agency shall require each person doing business with that agency to furnish to that agency such person's taxpayer identifying number."

Further, this information is provided consistently with the restrictions required by 5 U.S.C. 552a (Privacy Act of 1974) for individuals supplying information for inclusion in a system of records.

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

The implementation of this system, including activities such as the collection of PII necessary for operating it, are authorized by 5 U.S.C. 301. 42 U.S.C § 3502 creates the Office of the Assistant Secretary for Administration (ASA) at HHS, and among the duties delegated to the ASA are oversight of these services, which are necessary to developing and maintaining a workforce.

31 U.S.C. 66a; 5 U.S.C. 5501 et seq., 5525 et seq., 5701 et seq., and 6301 et seq.; Executive Order 9397; Pub. L. 100-202, Pub. L. 100-440, and Pub. L. 101-509

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.

09-40-0010 Pay, Leave, & Attendance Records

09-90-0018 Personnel Records in Op. Offices

Identify the sources of PII in the system.

Online

Government Sources

Within OpDiv

Other HHS OpDiv

Other Federal Entities

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

The ITAS data is secured-FTP over to our Mainframe system, hosted by the NIH/CIT Data Center where it is processed with other HHS OPDIVs time and attendance data. That data is then shared with the Department's payroll provider Defense Finance and Account System (DFAS)

Other Federal Agencies

With DFAS to process payroll for HHS employees

Also with FDA which uses the information to load up their legacy systems for reporting and budget purposes.

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

Interconnection Security Agreements (ISAs) and/or Memorandums of Understanding (MOUs) exist for all ITAS data files (interfaces) provided to OpDivs and agencies such as DFAS and FDA

Describe the procedures for accounting for disclosures.

Disclosures from this system are unlikely to be made, except in furtherance of the primary purpose of the system. However, under section (c) of the Privacy Act of 1974, if any disclosures are made for certain described purposes (those listed under section (b)(2) through (b)(12) of the Act), the system owner or other individual to whom responsibility is assigned would need to maintain a record in a designated file concerning that disclosure. The disclosures that would require this accounting include disclosures made for routine uses ((b)(3)), to a recipient of records that have been rendered not individually identifiable for statistical research or for a reporting record ((b)(4)), to another United States government agency or organization working on behalf of the government for a civil or criminal law enforcement activity ((b)(7)); to either House of Congress or Congressional committee working within its authority ((b)(9)); or pursuant to a court order ((b)(11)).

HHS is aware of this requirement and will keep an accounting of disclosures as required in a designated file. Information retained, as required, will include who made the request; exactly what information on each individual was provided; and the date of the disclosure. These records will be maintained for the period of time required (at least five years after the disclosure or for as long as the individual's record is maintained, whichever is longer). HHS will also comply with its requirement to make this record available to the individual on request, unless an exception or exemption applies.

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 occur as part of the Human Resources (HR) employee hiring and on-boarding process.

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 would be notified directly of major system changes that affect their rights or interests, but no such changes are anticipated. Major changes would also be reflected by updates to the system of records notice (SORN).

Information is collected from individuals. Consent is granted as part of the employee induction process.

Use of this data is implicit in the employer/employee relationship. Employees are expected to be aware that the business of HHS includes conducting analyses related to budgeting, staffing, and payroll.

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

Individuals would be notified directly of major system changes that affect their rights or interests, but no such changes are anticipated. Major changes would also be reflected by updates to the system of records notice (SORN).

Notice of any system changes is given to OPDIV leads during User Acceptance Testing (UAT) and consent is obtained from these representatives upon completion of UAT. An All Points Bulletin is sent out to all ITAS Users (Timekeepers, Admin officers, LAOs) with the release notes for this system change.

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.

ITAS maintains data for federal and civilian HHS employees. All formal and informal federal procedures are available for queries and concerns. Individuals may request assistance from supervisors, HR offices, Help Desk lines, or Information Security Officers, all of which would ultimately lead to correction or mitigation.

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

Employee data are changed by Human Resources personnel at the request of individuals, or by the individual employee. PII data critical to employee payroll are reviewed prior to submission to payroll process on biweekly basis, and corrected if necessary.

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

Users:

Data entry

Administrators:

on-boarding employees, maintenance of leave balances etc.

Contractors:

For performing development/administration functions

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

Access is restricted using an authorization process. Only privileged users with administrative rights can access PII.

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 rights are determined by need to know basis when the user request access. Annual recertification process is conducted to make sure user roles have not changed.

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.

Information Systems Security Awareness and Privacy Awareness trainings are required annually. Rules of behavior must be acknowledged and signed before access is granted.

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

Training on the use of the system is provided to supervisors as part of supervisor 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.

Retention and disposal practices are performed in concordance with the HHS Cyber Security Program Policy.

Records are retained and disposed of in accordance with National Archives and Records Administration's (NARA) General Records Schedule 2 (GRS 2), "Payrolling and Pay Administration Records," which prescribes retention periods ranging from as short as a few months or years to as long as 56 years. When an employee is separated, leave records are incorporated into the Official Personnel File (OPF) maintained by the servicing personnel office (SPO), and payroll retirement information is transferred to the Federal Retirement Records Center in Boyers, Pennsylvania. The OPF is forwarded to the new employing agency by the SPO. These procedures are in accordance with U.S. Office of Personnel Management policies and procedures.

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

Access is granted via AMS Simplified Sign On (SSO). Granting ITAS Coordinator privileges is done centrally by the ITAS administrator.

The following administrative, technical, and physical controls are in place for ITAS:

Administrative Controls

System security plan

Contingency (or backup) plan

File backup

Backup files stored offsite

User manuals

Security Awareness Training

Contractor Agreements

Least Privilege Access

PII Policies

Technical Controls

User Identification and Passwords

Firewall

Encryption

Intrusion Detection System (IDS)

Physical Controls
Guards
Identification Badges
Key Cards

The system is also secured by methods prescribed in the System Security Plan (SSP). The SSP calls for system life-cycle practices for Federal financial systems. The methods employed include risk assessments and implementation of management, operational, and technical controls.

In the Certification and Accreditation (C&A)process, the HHS Consolidated Acquisition Solution (HCAS) used NIST 800-53 security controls and established the required level of security measures, including end user IDs, passwords, group accounts, a certified facility, background screening on system administrators. Security controls will be reviewed annually, at a minimum.

Access to the system is controlled by two-factor authentication (PIV cards and iris scans), as well as 24x7 security guards at the perimeter, video surveillance that is monitored by the security guards, and there is always a member of the data center operations team (DCOB) within the data center control room. The rack which houses the servers is locked and the key is held by DCOB.

All access to the data center is tracked and logged in a central monitoring system. Visitors entering the data center are required to sign in (by way of a log book held and maintained by the security guards). In the log book you must specify name, organization, number, badge ID (if available), and time in/out.