US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

09/12/2016

OPDIV:

FDA

Name:

Administrative Applications: EASE and Associated Applications

PIA Unique Identifier:

P-3327697-164923

The subject of this PIA is which of the following?

Minor Application (child)

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?

New

Does the system have Security Authorization (SA)?

Yes

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

Describe the purpose of the system.

This PIA addresses FDA's Enterprise Administrative Support Environment (EASE) and the following additional applications:

Automated Employee Entrance Process (eArrive) is the web-based system used by the FDA to standardize the onboarding procedures for all new hires. The system is designed to enable completion of the onboarding process by the time they report for duty at FDA. eArrive is used to address the following needs of new FDA hires: Issuance of a Personal Identity Validation (PIV) card (FDA badge); establishing an FDA network account; creating an FDA e-mail address; and providing an opportunity to complete IT security awareness training.

Automated Employee Entrance Process Exit Process (eDepart) is a web-based application designed to assist the agency with meeting its requirements for employees, contractors and non-FDA government employees that are leaving the Agency.

Reporting and Management (RAM) is a tool used by budget staff responsible for tracking, approving and reporting on the annual funding provided to Centers (FDA component subagencies) with FDA. It is a data warehouse that draws funding information for Centers and Offices from EASE and uses the Business Objects web tool to create and run reports on organizational data, broken out by office and pay period. It does not access, collect or use PII.

Security: Used to provide Personal Identity Verification (PIV) badges to FDA staff and contractors and for background clearance purposes.

Help Desk: This Help Desk permits senior AdminApps administrators to provide roles and levels of access for administrators of specific applications. It centralized the function of awarding role-based access to AdminApps applications.

Users are FDA employees (and not, currently, contractors). Data subjects do not have access to their own HR files, although they will have access to eArrive in order to take the required Security training prior to having access to FDA systems.

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

The FDA Enterprise Administrative Support Environment (EASE) is a database containing information about FDA staff members. The EASE component is an FDA-wide administrative system that provides essential personnel, organization, and locator information, automates time and attendance processes, and provides ad hoc reporting capability through its associated data warehouse.

These applications store data sent from personnel systems related to employees and contractors, including any information that would be relevant to internal functions, including work and home contact information (phone, address, e-mail); unique identifiers including social security number and HHS employee ID number; and dates of employment or contract work. Any systems supplying information to EASE (such as Enterprise Human Resource Processing system (EHRP) and the Commissioned Corps system) are beyond the boundaries of this system and covered by other PIAs. EASE sends data to additional systems, as well, such as the Ethics system, that are covered in other PIAs.

eArrive and eDepart may additionally contain information about FDA-owned equipment issued or returned; badging status; access granted or revoked to networks, systems, or offices; parking privileges; and mandatory trainings assigned and/or completed.

RAM uses organizational budget data, broken out by office and pay period. It does not access, collect or use PII.

Security may contain information concerning the status of individuals' background checks; levels of clearance; access to facilities granted; and fingerprints.

Help Desk contains names of FDA staff with administrative roles; information about the subagency (center) and division for whom the individual works; and levels of access granted.

Help Desk additionally stores authentication information (usernames and passwords). None of the other applications in this PIA have this information, using instead a single sign on (SSO) multi-factor authentication approach to authorization and authentication.

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

EASE holds essential personnel, organization, and locator information, automates time and attendance data, and maintains a data warehouse to enable the production of ad hoc reporting materials.

eArrive is used to standardize the onboarding procedures for all new hires, including by issuing a Personal Identity Validation (PIV) card; establishing an FDA network account; creating an FDA e-mail address; and providing an opportunity to complete IT security awareness training.

eDepart is used to assist FDA in meeting requirements for employees, contractors and non-FDA government employees that are leaving the Agency. It uses PII to identify employees that are exiting the agency and track progress against offboarding tasks such as issuing final paychecks, requiring the return of loaned equipment, and establishing the last day of employment.

Reporting and Management (RAM) is a tool used by budget staff. It creates and runs reports on organizational data, broken out by office and pay period. It does not access, collect or use PII.

Security provides Personal Identity Verification (PIV) badges to FDA staff and contractors and for background clearance purposes.

Help Desk permits senior AdminApps administrators to provide roles and levels of access for administrators of specific applications. It centralizes the function of awarding role-based access to AdminApps applications.

eArrive, eDepart, Security, and Help Desk may contain information on FDA staff members and about FDA-owned equipment issued or returned; badging status; access granted or revoked to networks, systems, or offices; parking privileges; and mandatory trainings assigned and/or completed.

Most of the information is accessed via EASE and does not reside within these other applications, butis instead accessed from EASE and passed through these other systems at the time the system is consulted or queried.

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

Date of Birth

Name

Biometric Identifiers

E-Mail Address

Mailing Address

Phone Numbers

Education Records

Military Status

Employment Status

Foreign Activities

Passport Number

HHS employee identification numbers

Systems, networks and facilities to which the individuals have been granted access

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

Employees

Public Citizens

Vendor/Suppliers/Contractors

"Public citizens" refers to selected job applicants for whom the onboarding process is not concluded. Once onboard, they are employees.

How many individuals' PII is in the system?

10,000-49,999

For what primary purpose is the PII used?

All applications addressed in this PIA (except RAM) use PII to conduct administrative human resources related functions, including tracking employees and contractors and ensuring they are satisfying privacy and security requirements that are conditions of their employment and conducting onboarding and offboarding activities.

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

None.

Describe the function of the SSN.

SSN is used to identify individuals uniquely when required by law (or when for any reasons identification is not otherwise possible). For example, as explained later in this document, use of the SSN is required to conduct certain security functions, such as background checks.

Cite the legal authority to use the SSN.

Use of Social Security numbers is supported by Executive Order 9397, as amended.

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

Use of Social Security numbers is supported by Executive Order 9397, as amended.

Personnel security functions required by the Security application as well as some functions of eArrive and eDepart are supported by Homeland Security Presidential Directive (HSPD) 12, which required in part that "the Secretary of Commerce shall promulgate in accordance with applicable law a Federal standard for secure and reliable forms of identification" to "enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy."

General authority for implementing regulations for the usual and necessary infrastructure of running an organization is provided to agencies by 5 United States Code (U.S.C)301. These systems enable fundamental business practices such as hiring, separating departing employees, providing employees access to resources, and protecting infrastructure.

These systems support the necessary function of identifying, evaluating, and employing staff with appropriate knowledge, skills and abilities, an activity authorized generally by 5 U.S.C. Sec. 3101, "General authority to employ: Each Executive agency, military department, and the government of the District of Columbia may employ such number of employees of the various classes recognized by chapter 51 of this title as Congress may appropriate for from year to year." Other authorities related to the use and disclosure of employment-related information can be found in 5 U.S.C. Part III.

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.

NOTE: Four applications (eArrive, eDepart, EASE, and Security) addressed in this PIA are subject to

SORN 09-90-0777, Facility and Resource Access Control Records

SORN 09-90-0018, Personnel Records in Operating Offices

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Hardcopy

Email

Online

Government Sources

Within OpDiv

Identify the OMB information collection approval number and expiration date

OMB information collection approval is in progress. OMB approval may be necessary for eArrive and Security. The system point of contact is coordinating with the office responsible for requesting information collection approval numbers and initiate the approval process.

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.

Individuals submit most information themselves at the time of collection as part of the hiring and onboarding process. Individuals are further aware of additional information generated (e.g., that equipment has been assigned to them or that a background clearance has been conducted) because they participate directly in the 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.

Employment at FDA is voluntary; however, the information is mandatory to appropriately clear employees and contractors; award them appropriate access; and conduct necessary functions such as tracking the provision of mandatory training, track computers and other equipment assigned, issue PIV badges, and others.

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

If the agency changes the collection, use, or sharing of PII data in this system, the affected individuals will be notified by the most efficient and effective means available and appropriate to the specific change(s). This may include a notice on an FDA web site, e-mail notice to the individuals, inclusion in newsletters, or information provided to supervisors with instructions to further inform staff. However, no such changes that would affect the rights or interests of the individuals are anticipated.

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.

Applicants may address any such issues by contacting the FDA coordinator of the program or activity for which they are working or using general FDA contact information. Any such concerns would be reported to appropriate parties which may include the system administrator, the Computer Security Incident Response Team, or a Help Desk. Any changes to an individual's name or address would need to be updated using a Standard Form 50 or 52, which is required for all such changes for FDA employees, and the data would be updated in FDA's human resources information system, CapHR.

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

EASE receives electronic updates nightly from HHS' Enterprise Human Resource Processing system (EHRP) with official data on all active FDA civilian personnel and receives similar updates nightly from the Commissioned Corps personnel system. The primary key between EHRP, the Commissioned Corps system and EASE is SSN. This data flows one way; EASE does not send data to the EHRP or the Commissioned Corps system.

Individuals who are not yet FDA employees are responsible for supplying correct information. FDA offices verify that correct information has been supplied at the time of new employee onboarding.

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

Users:

"Users" are FDA employees that have access to the various applications to perform FDA administrative functions, not the data subjects themselves Require full access to systems in order to conduct activities related to onboarding and hiring, providing access to systems and networks, and other administrative activities Note that "users" may include subject individuals, supervisors, or business function administrators.

Administrators:

Administrators may be application administrators who require access to conduct business functions, or application administrators who require access in order to create and manage user accounts for specific applications.

Developers:

Developers will not normally have access to PII, but may in the course of maintaining the systems or providing technical assistance.

Contractors:

Some developers may be direct contractors and will have access under the same circumstances as developers.

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

For all applications, administrative access to EASE is granted by existing system administrators. New users seek administrative access when assigned duties requiring this access. Employees then coordinate with applications administrators who in turn inform employees of how to log on and what actions must be taken. The user's supervisor uses an account creation form to specify the minimum information system access that is required in order for the user to complete required tasks.

Subject individuals do not have direct access to their EASE accounts, but request corrections and updates using a link on the FDA Intranet homepage or through a number of other routes, such as working through supervisors or calling a technical help line.

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.

Management establishes roles for individual personnel, with role-based restrictions permitting access only to information that us required for each individual to perform his/her job.

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 personnel/users are required to complete FDA's IT Security and Privacy Awareness training at least annually.

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

A user manual is available that walks the user through each step and functionality of many of these applications. For example, manuals for eArrive and eDepart are freely available and conspicuously linked on the FDA Intranet. These provide guidance for subject individuals as well as administrators that create accounts. The other applications have documentation as well, and plans are in place as of September 2014 to post these on the FDA intranet.

All users are instructed on adhering to the HHS Rules of Behavior in the context of their work involving this system. For additional privacy guidance, personnel may contact the agency's privacy office. Privacy program materials are provided to personnel on a central intranet page. Personnel may take advantage of information security and privacy awareness events and workshops held within FDA.

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.

For the EASE database itself, records are maintained by a schedule in the FDA 9110 File Code series, specific to EASE, including File Codes 9111 through 9117 inclusive. 9111 covers Inputs (Core and Other Data), which is to say, data that may be updated by newer information provided by the EHRP system, at which time the previous data may be overwritten and destroyed.

All other applications in this are maintained under General Records Schedule (GRS) 3.2, Information Systems Security Records; Item 030, System Access Records. This schedule is for “records created as part of the user identification and authorization process to gain access to systems.” Disposition for these files is temporary, and the files may be destroyed/deleted when business use ceases. If the application owner determines that an application requires special accountability, retention may be six years after the password is altered or the user account is terminated, and 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.

Administrative Safeguards include training and awareness provided for all users; system manuals that advise on the systems' proper use; implementation of Need to Know and Minimum Necessary principles when awarding access, and others. Technical Safeguards include that PII entered via these systems is immediately pulled through the web-based systems into the systems that are internal and not connected to the web, removed from the public site, and not accessible to others submitting information via these systems or fda.gov. Physical controls include that all system servers are located at FDA facilities protected by guards, locked facility doors, and climate controls. Appropriate controls have been selected from the National Institute of Standards and Technology’s (NIST’s) Special Publication 800-53 as determined using Federal Information Processing Standard (FIPS) 199.