PTA / PIA: FDA - CAAPS - QTR2 - 2025 - FDA4933516

Created Date: 6/6/2025 12:28 PM Last Updated: 6/24/2025 4:45 PM

General Information

PTA / PIA Name:	FDA - CAAPS - QTR2 - 2025 - FDA4933516	**PTA / PIA ID:**	3279059
Component Name:	FDA - CDRH Acquisition & Administrative Planning System Human Resources Position Based Management	**ATO Boundary Name:**	CDRH Center Engagement and Workforce Development
Overall Status:	Complete	**# of Days - Open:**	18
Submitter:		**Submit Date:**	6/6/2025
Next Assessment Date:	N/A	**Expiration Date:**	1/1/2100
Office:		**OpDiv:**	FDA
Security Categorization:	Moderate		
Make PIA available to Public?:	No	**PIA Required:**	Yes

General 01:	Identify the Enterprise Performance Lifecycle Phase of the system.	Operations and Maintenance
General 02:	Is this a FISMA-Reportable system?	Yes
General 03:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	No
General 04:	ATO Date or Planned ATO Date.	8/18/2023
General 05:	Is the system or electronic information collection, agency or contractor operated?	Agency
History Log:	View History Log	

Privacy Threshold Analysis

Privacy Threshold Analysis

PTA 01:	Point of Contact (POC) Name	Anjila Merchant
PTA 01A:	POC Title and Organization	Program Manager, CDRH/OST/IO
PTA 01B:	POC Email Address	anjila.merchant@fda.hhs.gov
PTA 01C:	POC Phone Number	301-802-4697
PTA 02:	Indicate the following reason(s) for this PTA. Choose from the following options.	PIA Validation (PIA Refresh)

PTA 02A:	Describe in further detail any changes to the system that have occurred since the last PIA.	FDA has made no changes to this [system/component/information collection] since the last Privacy Threshold Analysis/Privacy Impact Assessment was approved.
PTA 03:	Is the data contained in the system owned by the agency or contractor?	Agency
PTA 04:	Please give a brief overview of the purpose of the system by describing what the functions of the system are and how the system carries out those functions in support of HHS.	The purpose of the Food and Drug Administration (FDA) Center for Devices and Radiological Health (CDRH) HR – Position Based Management (HR-PBM) system ("HR" is used in the system name to reflect the Human Resources nature of the system) is to provide a custom application designed to support the workforce functions and internal support services provided by the CDRH Office of Management, Division of Workforce Management (DWM, the system user organization) to CDRH HR-PBM users. The system provides the ability to create, review, manage and execute recruitment packages, personnel action request (PAR) actions, and position and employee profiles (i.e., profiles containing information about current or former CDRH Federal employees and CDRH positions). CDRH HR-PBM is operated by FDA employees and/or FDA Direct Contractors. No external third-party operates, supports, uses or has access to the system.

PTA 05:	List and/or describe all the types of information that are collected, maintained, and/or shared by the system regardless of whether that information is PII and how long that information is stored.	The HR-PBM system collects and stores human capital management information related to the creation, review, management and execution of recruitment packages, personnel action request (PAR) actions, and position and employee profiles. The PII data elements in HR-PBM and sources of each element are as follows: (1) Name (data sources: Enterprise Human Capital Management (EHCM), Enterprise Administrative Support Environment (EASE), HR-PBM system manual entry) (2) Work and personal email addresses (data sources: EHCM, EASE, HR-PBM system manual entry) (3) Work and personal phone numbers (data sources: EHCM, EASE, HR-PBM system manual entry) (4) Employment status (data sources: EHCM, EASE, HR-PBM system manual entry) (5) U.S. Department of Health and Human Services (HHS) ID (data source: EHCM) (6) EHCM Employee ID (data source: EHCM) (7) EHCM Position ID (data source: EHCM) (8) EASE ID (a unique alphanumeric identifier; data source: EASE) (9) Social Security number [SSN] (data sources: EASE, EHCM) (10) Military status (Data Source: HR-PBM system manual entry) (11) Medical notes (applicant disability documentation) (Data Source: HR-PBM system manual entry) (12) Certificates (Data Source: HR-PBM system manual entry) (13) Date of Birth (data sources: EHCM, EASE, HR-PBM system manual entry) (14) Photographic Identifiers (data sources: EASE, HR-PBM system manual entry) (15) Education Records (Data Source: HR-PBM system manual entry) (16) Work and home mailing addresses (data sources: EHCM, EASE, HR-PBM system manual entry) The system retains PII for different periods under applicable record schedules described in this assessment. The system uses a Single Sign-on (SSO) process for user authentication and access and does not require users to enter PII such as a username or password for authentication.
PTA 05A:	Are user credentials used to access the system?	Yes, but the user credentials are maintained in a separate system (e.g., AD, AMS) and not collected or maintained by this system.
PTA 05C:	Please identify the system that maintains the user credentials or controls access to this system.	Active Directory
PTA 06:	Describe why each type of information is collected, maintained, and/or shared by the system. Specify what information is collected about each category of individual.	The HR-PBM system is used by CDRH Human liaisons (referred to as users) to create, review, recruitment packages, personnel action

request actions, and position and employee profiles. Human HR-PBM is received from the Department of (HHS) Enterprise Human Capital Management the HHS Business Intelligence Information System Enterprise Administrative Support Environment and EASE are the immediate sources of the system. EASE provides information about current of name, SSN, EASE ID, work phone number, work email address, and employee provides name, SSN, EHCM ID, EHCM Employee ID, work phone number, work email address, and employee upstream systems are the subject of separate obtained from them is aligned with the purposes collected into the source systems.

The HR-PBM system provides data entry screens system position and employee information. It functions enabling users to upload documentation for packages.

For purposes of position management, HR liaisons screens in the HR-PBM system to add positions data is received from the EHCM and EASE system extracts.

For HR Actions, HR liaisons use data entry screens for new personnel requests and new recruitment requests. HR liaisons use government source systems within the FDA to view and add the following PII about federal employees working at CDRH to the HR-PBM system. This is done by manual data entry via data entry screens in HR-PBM. The PII entered in this manner is first and last name, work email address, work phone number, and employment status. HR liaisons also have the option to upload documentation to the system as attachments for job application packages. The PII in the attachments is about current federal employees applying for CDRH positions and individuals not employed by the Federal government applying for a CDRH position. The PII about employees and individuals not employed by Federal government who apply for CDRH positions may include contact information, work details, military status (if applicable), educational certificates (if applicable), and medical notes (i.e., letter to document applicant disability to qualify for Schedule A hiring authority).

Social Security number (SSN) is used in the automated extraction, transformation and load (ETL) process to accurately merge and match CDRH federal employee data from EASE and EHCM to source data for HR-PBM. The SSN data is stored in the backend database staging tables only and is not visible to users in the front-end of the application.

There is no information shared back from HR-

		PBM to EHCM or EASE. When HR liaisons identify incorrect position or employee data in HR-PBM, they formally submit corrections to the EHCM and EASE record administrators. SSN is not transmitted in any instances of performing a record correction and as described in this assessment, is not visible to the user in the front-end of the application. There is no use of a mobile application with HR-PBM. The system does not employ any system-specific access credentials (username, password). Access and user authentication are executed through a single sign-on (SSO), network-level multifactor authentication process. CDRH HR-PBM personnel who access or use the system utilize personal identifiers to retrieve records held in the system. Within the HR-PBM user interface, CDRH personnel use PII to retrieve information from HR-PBM (not from a source system or other system separate from HR-PBM) about current federal employees working at CDRH. The PII used for retrieval actions includes HHS ID, first name, last name, and email address (work) about federal employees only. FDA does not use PII about non-federal employees/individuals to retrieve records in the system.
PTA 07:	Does the system collect, maintain, use, or share PII?	Yes
PTA 08:	Does the system include a website or online application?	Yes
PTA 08A:	Provide the URL(s).	https://cdrhcaaps.fda.gov/app/
PTA 08B:	Are any of the website or online applications accessible by the public (including publicly accessible log in pages)?	No
PTA 09:	Describe the purpose of the website, who has access to it, and how users access the web site (via public URL, log in, etc.). Please address each element in your response.	The purpose of the website is to allow CDRH HR-PBM users the ability to create, review, manage and execute recruitment packages, personnel action request (PAR) actions, and position and employee profiles (i.e., profiles containing information about current or former CDRH Federal employees and CDRH positions). CDRH HR-PBM is operated by FDA employees and/or FDA Direct Contractors. No external third-party operates, supports, uses or has access to the system. Access and user authentication are executed through a single sign-on (SSO), network-level multifactor authentication process.
PTA 10:	Does the website have a posted privacy notice?	Yes
PTA 11:	Does the website contain links to non-federal government websites external to HHS?	No
PTA 12:	Does the website use web measurement and customization technology?	No
PTA 13:	Does the website have any information or pages directed at children under the age of thirteen?	No

PTA 14:	Does the system have a mobile application?	No
PTA 20:	Are any third-party websites or applications (TPWA) associated with the system?	No
PTA 21:	Does this system use artificial intelligence (AI) tools or technologies?	No

Privacy Impact Assessment

Privacy Impact Assessment

PIA 22:	Indicate the type(s) of personally identifiable information (PII) that the system will collect, maintain, or share.	Identifying Numbers Social Security Number Biographical Information Name Date of Birth Certificates (e.g., training certificates) Education Records Employment Status/History Military Status/History Contact Information Email Address (Personal) Mailing Address (Personal) Phone Numbers (Personal) Email Address (Business) Mailing Address (Business) Phone Numbers (Business) Biometrics/Distinguishing Features Photographic Identifiers Medical Information Medical Records Other Other
PIA 22A:	Identify the “other” type(s) of personally identifiable information (PII) not mentioned in the above list.	HHS ID EHCM Employee ID EHCM Position ID EASE ID
PIA 23:	Indicate the categories of individuals about whom PII is collected, maintained, or shared.	Employees/HHS Direct Contractors
PIA 24:	Indicate the approximate number of individuals whose PII is maintained in the system.	500 – 4,999
PIA 25:	For what primary purpose is the PII used?	Authorized personnel use the PII in the HR-PBM application to manage Federally funded positions and identify services for Personnel Action Requests (PAR) for Federal employees. PII is also used for position management, vacancy forecasting and help with processing PAR requests on behalf of center employees. HR-PBM uses FDA’s Single Sign-On (SSO) environment and does not require users to enter PII information for authentication.

PIA 26:	Describe any secondary uses for which the PII will be used (e.g., testing, training, or research).	Not applicable (N/A). There is no secondary usage (training, testing, research) of the PII in the system.
PIA 27:	Describe the function of the SSN, Truncated SSN, and/or Taxpayer ID. If the Taxpayer IDs collected are only for businesses include that in your response.	SSN is not collected from individuals but is obtained from other systems (HHS EHCM and FDA EASE) to ensure data accuracy. Data integrity and accuracy processes involve use of SSN to avoid data merge errors and, ensure data is associated with the correct subject. For this purpose, SSN is used only in the backend database staging tables to merge data from the HHS EHCM and FDA EASE source systems. SSN is not visible to or accessible by the users in the front-end of the application. These merging and accuracy steps are automated; users do not manually compare SSNs.
PIA 27A:	Cite the legal authority to use the SSN, Truncated SSN, and/or Taxpayer ID. If the Taxpayer IDs collected are only for businesses, you may respond N/A.	5 U.S.C. 8347 and Executive Order 9397 as amended. Note that SSN is not collected from individuals into HR-PBM. It is received by HR-PBM from the HHS EHCM and FDA EASE source systems.
PIA 28:	Identify legal authorities, governing information use and disclosure specific to the system and program.	5 U.S.C. 301, 2105, 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, as amended by 13478, 9830, and 12107.
PIA 29:	Are records in the system retrieved by one or more PII data elements?	Yes
PIA 29A:	Please specify which PII data elements are used to retrieve records.	The PII used for retrieval actions includes HHS ID, first name, last name, and email address (work) about federal employees only.
PIA 29B:	Provide the number, title, and URL of the Privacy Act System of Records Notice (SORN) that is being used to cover the system or indicate whether a new or revised SORN is in development.	OPM/GOVT-1 General Personnel Records
PIA 30:	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains Email Government Sources Within the OPDIV
PIA 31:	Is there an Office of Management and Budget (OMB) information collection approval number?	No
PIA 31B:	Explain why an OMB information collection approval number is not required.	The system does not entail an information collection subject to the Paperwork Reduction Act.
PIA 32:	Is the PII in the system shared directly with other organizations outside the system's Operating Division?	No
PIA 33:	Is the submission of PII by individuals voluntary or mandatory as defined in the Privacy Act?	Voluntary

PIA 34:	Describe the method in place to notify and obtain consent from individuals whose PII will be collected. If no prior notice is given or consent cannot be obtained, explain why.	There is no system-specific opt-out process. CDRH uses the PII handled by HR-PBM internally for human capital management purposes. Individuals seeking to opt-out may contact the offices managing the source systems, use HHS EHCM and/or FDA EASE employee help desk resources, or obtain assistance from other offices such as the FDA Privacy Office. Applicants may opt not to apply for a position.
PIA 35:	Describe the process to notify and obtain consent from the individuals whose PII is in the system when major changes occur to the system (e.g., disclosure and/or data uses have changed since the notice at the time of original collection). If they cannot be notified or have their consent obtained, explain why.	The PII in HR-PBM comes via automated processes from HHS EHCM and FDA EASE as well as from manual entry of content from job application materials. If a change occurs in the way PII is handled, the source system administrators would conduct notification of individuals of the change. For PII manually entered in the system, HR-PBM administrators would notify individuals via email or correspondence if any major changes occur to how the PII is handled.
PIA 36:	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. If no process exists, explain why not.	The information in HR-PBM comes via automated transmission from HHS EHCM and FDA EASE and manually pulled from job application documents and manually entered in HR-PBM by HR liaisons via data entry screens. Individuals with concerns regarding their PII may contact officials for HR-PBM, HHS EHCM and FDA EASE. Employees may also report suspected data breaches and obtain assistance through FDA's Employee Resource Information Center (ERIC), FDA's Cybersecurity Infrastructure Operations Coordination Center (CIOCC), and Privacy Office. HHS and FDA policy obligates all permanent and Direct Contractor personnel to report suspected breaches. Within FDA, all reports of suspected breaches must be reported to the CIOCC.

PIA 37:	Describe the process in place for periodic reviews of the system to ensure the integrity, availability, accuracy, and relevancy of the PII in the system. Please address each element in your response. If no processes are in place, explain why not.	As the primary source of PII in HR-PBM, the HHS EHCM and FDA EASE systems and their operators are responsible for primary maintenance of PII integrity, accuracy, availability and relevancy. FDA loads human capital data (which contains PII) in HR-PBM, and a report is produced flagging discrepancies. An HR liaison submits corrections to the source system owner to have corrections made. The source system will then transmit the corrections to HR-PBM. CDRH reviews the system access list and restrictions on a quarterly basis during which time users' access permissions are reviewed / adjusted and unnecessary accounts and permissions are identified and removed or adjusted. HR liaisons with access to the system conduct reviews on a regular basis to review the PII and confirm accuracy and data integrity. SSN is used to support PII accuracy by merging the data from the EHCM and EASE source systems (associate it with the correct individual). PII relevancy is supported by system design that obtains only the essential PII from the source systems. PII integrity and availability are supported by technical and administrative security and privacy controls outlined in guidance issued by the National Institute of Standards and Technology (NIST), as well as by continuing operations plans and procedures (e.g., data backups).
PIA 38:	Identify who will have access to the PII in the system.	Users Administrators Developers Contractors
PIA 38A:	Select the type of contractor.	HHS/OpDiv Direct Contractors
PIA 38B:	Do contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices?	Yes

PIA 39:	Provide the reason why each of the groups identified in 38 needs access to PII.	Users: Users create, review, manage and execute recruitment packages, personnel action request (PAR) actions, position and employee management. Administrators: For System Administration within HR-PBM. Developers: For System Development within HR-PBM. Contractors: Direct Contractors have access to this data for system administration and development work to address FDA's business needs.
PIA 40:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	All access to HR-PBM require supervisor approval prior to the user gaining access. Systems access is reviewed on a quarterly basis to identify and remove unnecessary accounts.
PIA 41:	Describe the technical methods in place to allow those with access to PII to access only the minimum amount of information necessary to perform their job.	Access for system administration is limited to a work need basis. Administrators are subject to a higher level of background check. CDRH revises the access list and restrictions are reviewed on a quarterly basis during which time users' access permissions are reviewed/adjusted and unnecessary accounts and permissions are identified and removed or adjusted.
PIA 42:	Identify the general security and privacy awareness training provided to system users (system owners, managers, operators, contractors and/or program managers) to make them aware of their responsibilities for protecting the information being collected and maintained.	All personnel, including Direct Contractors complete Security and Privacy Awareness training at least annually.
PIA 43:	Describe the training system users receive above and beyond general security and privacy awareness training.	No additional system-specific training is provided. Personnel may contact FDA's privacy staff for guidance.

PIA 44:	Describe the process and guidelines in place for the retention and destruction of PII. Cite specific National Archives and Records Administration (NARA) records retention schedule(s) and include the retention period(s).	The data retention and destruction practices for HR-PBM adhere to the guidance in the Administrative Schedule – FDA 9990: Information Technology, Electronic Records. System records, including employee data, are addressed in Section 9995e, Downloaded and Copied Data, i.e., "Derived data and data files that are copied, extracted, merged, and/or calculated from other data generated within the agency, when the original data is retained." Disposition for this data is TEMPORARY. It can be deleted when no longer needed. The following National Archives and Records Administration (NARA) schedules apply to records, including those containing PII, in HRPBM: GRS 2.1 Employee Acquisition Records 050: Job vacancy case files (Records of one-time competitive and Senior Executive Service announcements/selections): Disposition Instructions: Destroy 2 years after selection certificate is closed or final settlement of any associated litigation; whichever is later. 051: Job vacancy case files (Records of standing register competitive files for multiple positions filled over a period of time): Disposition Instructions: Temporary. Destroy 2 years after termination of register. 060: Job application packages: Disposition Instructions: Temporary. Destroy 1 year after date of submission. 110: Excepted service appointment records (Case files that document appointing individuals with intellectual disabilities, severe physical disabilities, or psychiatric disabilities as defined in 5 CFR 213.3102(u)): Disposition Instructions: Temporary. Destroy 5 years after candidate enters on duty, is no longer under consideration, or declines offer.
PIA 45:	Describe how the PII will be secured in the system using administrative, technical, and physical controls. Please address each element in your response.	Administrative safeguards include user training; system documentation that advises on proper use; implementation of Need to Know and Minimum Necessary principles when awarding access, and others. Technical safeguards include role-based access settings, firewalls, passwords and others. Physical controls include that all system servers are located at FDA facilities protected by guards, locked facility doors, and climate controls. Other 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.

Review and Comments

OpDiv Privacy Analyst Review

Privacy Analyst Review Decision:	Approved	**Privacy Analyst Review Date:**	6/6/2025
Privacy Analyst Review Comments:		**# of Days - PA Review:**	0

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	6/6/2025
SOP Review Comments:	The FDA's Senior Official for Privacy (SOP) has: (a) approved the Privacy Threshold Analysis (PTA)/Privacy Impact Assessment (PIA) conducted for the subject system/component; (b) reviewed and approved the associated security categorization; and (c) reviewed and confirmed acceptable implementation status of the assigned privacy controls.	**# of Days - SOP Review:**	0

Agency Privacy Analyst Review

Agency Privacy Analyst Review Decision:	Approved	**Agency Privacy Analyst Review Date:**	6/10/2025
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte 6/10/2025 This PIA is ready for SAOP review and approval.	**# of Days - APA Review:**	4

SAOP Review

SAOP Review Decision:	Approved	**SAOP Review Date:**	6/24/2025
SAOP Review Comments:		**# of Days - SAOP Review:**	14

SAOP Signature

Date	User	Type	Name	Original Value	New Value
6/24/2025 3:24 PM	GUENTHER, BRIDGET	Signature	SAOP (Email PIN)		Content Signed

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
No Records Found				

Comments

Question Name	Submitter	Date	Comment	Attachment
PTA 01	BLAND, CRYSTAL	6/6/2025	Per FDA's Email: The attached PIA is SOP approved and should be in your queue. The PIA is experiencing an Archer error with question General 03: Q-3 “Does the system have or is it covered by a Security Authorization to Operate (ATO)?” o The FDA instance of Archer is automatically entering the answer “No,” which is incorrect. The ATO date is 8/18/2023. o At this time, we are unable to update Archer to reflect the correct answer “Yes.” The FDA Archer Team is aware of this occurrence and is working on a solution.	6-5-2025 EMAIL_PIA in Queue (CDRH Acquisition & Administrative Planning System).pdf CDRH Acquisition & Administrative Planning System HR-PBM_SOP Aprroved.pdf