Privacy Impact Assessment (PIA): FDA - CAAPS HR-PBM - QTR2 - 2022 - FDA2041729

Date Signed: 4/11/2022

Acronyms

ATO - Authorization to Operate
CAC - Common Access Card
FISMA - Federal Information Security Management Act
ISA - Information Sharing Agreement
HHS - Department of Health and Human Services
MOU - Memorandum of Understanding
NARA - National Archives and Record Administration
OMB - Office of Management and Budget
PIA - Privacy Impact Assessment
PII - Personally Identifiable Information
POC - Point of Contact
PTA - Privacy Threshold Assessment
SORN - System of Records Notice
SSN - Social Security Number
URL - Uniform Resource Locator

General Information

Status:	Approved	**PIA ID:**	1439669
PIA Name:	FDA - CAAPS HR-PBM - QTR2 - 2022 - FDA2041729	**Title:**	FDA - CDRH Center Engagement and Workforce Development
OpDIV:	FDA		

PTA

PTA - 1A:	Identify the Enterprise Performance Lifecycle Phase of the system	Implementation
PTA - 1B:	Is this a FISMA-Reportable system?	No
PTA - 2:	Does the system include a website or online application?	No
PTA - 3:	Is the system or electronic collection, agency or contractor operated?	Agency
PTA - 3A:	Is the data contained in the system owned by the agency or contractor?	Agency
PTA - 5:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	No
PTA - 5B:	If no, Planned Date of ATO	4/1/2021
PTA - 8:	Please give a brief overview and purpose of the system by describing what the functions of the system are and how the system carries out those functions?	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 - 9:	List and/or describe all the types of information that are collected (into), maintained, and/or shared in 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: EHCM, EASE, HR-PBM system manual entry) (2) Work email address (data sources: EHCM, EASE, HR-PBM system manual entry) (3) Work phone number (data sources: EHCM, EASE, HR-PBM system manual entry) (4) Employment status (data sources: EHCM, EASE, HR-PBM system manual entry) (5) 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) Mailing Address (data sources: EHCM, EASE, HR-PBM system manual entry) Please defer to the attached PIA - CDRH HR PBM PIA 3-15-2022 for further info related to this response.
PTA -9A:	Are user credentials used to access the system?	No

PTA - 10:	Describe why all types of information is collected (into), maintained, and/or shared with another system. This description should specify what information is collected about each category of individual	The HR-PBM system is used by CDRH Human Resources (HR) liaisons (referred to as users) to create, review, manage and execute recruitment packages, personnel action request (PAR) actions, and position and employee profiles. Human capital information in HR-PBM is received from the Department of Health and Human Services (HHS) Enterprise Human Capital Management (EHCM) database through the HHS Business Intelligence Information System (BIIS) and the FDA Enterprise Administrative Support Environment (EASE) database. EHCM and EASE are the immediate sources of the PII handled by the system. EASE provides information about current employees consisting of name, SSN, EASE ID, work phone number, work email address, and employee status. EHCM provides name, SSN, EHCM ID, EHCM Employee ID, HHS ID, work phone number, work email address, and employee status. These upstream systems are the subject of separate PIAs. CDRH's use of the PII obtained from them is aligned with the purposes for which the PII is collected into the source systems. The HR-PBM system provides data entry screens used to add to the system position and employee information. It also has an attachment function enabling users to upload documentation for job application packages. For purposes of position management, HR liaisons use data entry screens in the HR-PBM system to add positions and employees before the data is received from the EHCM and EASE system extracts. Due to exceeding character limit, please defer to the attached CDRH HR PBM PIA 3-15-2022 for further info related to this response.

PTA - 10A:	Are records in the system retrieved by one or more PII data elements?	Yes
PTA - 10B:	Please specify which PII data elements are used.	The PII used for retrieval actions includes HHS ID, first name, last name, and email address (work) about federal employees only
PTA - 11:	Does the system collect, maintain, use or share PII?	Yes

PIA

PIA - 1:	Indicate the type of PII that the system will collect or maintain	Social Security Number Name E-Mail Address Phone numbers Medical records (PHI) Certificates Education Records Military Status Date of Birth Photographic Identifiers Mailing Address Employment Status Others - HHS IDEHCM Employee IDEHCM Position IDEASE IDCertificates refers to educational records of current federal employees applying for CDRH positions and individuals not employed by the federal government applying for a CDRH position. All personal and professional contact information, professional work details are collected.
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared	Employees/ HHS Direct Contractors Public Citizens
PIA - 3:	Indicate the approximate number of individuals whose PII is maintained in the system	Above 2000
PIA - 4:	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 - 6:	Describe the function of the SSN/Taxpayer ID.	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 - 6A:	Cite the legal authority to use the SSN	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 - 7:	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 - 8:	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 - 9:	Identify the sources of PII in the system	Directly from an individual about whom the information pertains Online Government Sources Within the OPDIV Other HHS OPDIV
PIA - 10:	Is the PII shared with other organizations outside the system's Operating Division?	No
PIA - 11:	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 do not themselves enter or provide their information directly to CDRH or the HR-PBM system. The PII about them in the system is not something FDA or CDRH collect directly from the individual. The PII is

		obtained manually (e.g., viewing application documents stored outside HR-PBM and manually entering the data). CDRH's use of the PII is downstream from other FDA and HHS source systems. When required, officials administering source systems are responsible for providing notice to individuals, such as displaying a Privacy Act Statement on forms or web pages that collect PII to be maintained in a Privacy Act system of records. CDRH's use of the PII is aligned with the purposes for which the PII is collected into the source systems. The PII in HR-PBM comes from FDA's EASE and HHS EHCM systems. EHCM is operated by an HHS office external to FDA. As the source system owners, the EASE and EHCM programs notify individuals. At the time of hire, HHS/FDA provides notice of the collection, creation and use of PII to all personnel via forms and webpages and other materials used in the hiring and onboarding process. When logging on to the network as a preliminary step to access HR-PBM, all individuals must acknowledge a warning message advising them of the lack of privacy when using government systems and resources. FDA's website and privacy policies are posted on all FDA internet and intranet pages. The applicable SORN also provides notice, as does this PIA and the PIAs for the source systems. HHS and FDA webpages (internal as well as public-facing) and job announcements provide notice information and links to website and privacy policies.
PIA - 12:	Is the submission of PII by individuals voluntary or mandatory?	Voluntary
PIA - 13:	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	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 - 14:	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). Alternatively, describe why they cannot be notified or have their consent obtained	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 - 15:	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 Systems Management Center (SMC), and FDA's 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 SMC.
PIA - 16:	Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy. 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 - 17:	Identify who will have access to the PII in the system and the reason why they require access	Users Administrators Developers Contractors
PIA - 17A:	Provide the reason of access for each of the groups identified in PIA -17	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 - 17B:	Select the type of contractor	HHS/OpDiv Direct Contractor
PIA - 18:	Describe the administrative procedures in place to determine	All access to HR-PBM require supervisor approval prior to the user

	which system users (administrators, developers, contractors, etc.) may access PII	gaining access. Systems access is reviewed on a quarterly basis to identify and remove unnecessary accounts.
PIA - 19:	Describe the technical methods in place to allow those with access to PII to only access 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 - 20:	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, including Direct Contractors complete Security and Privacy Awareness training at least annually.
PIA - 21:	Describe 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 - 23:	Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific 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 HR-PBM: 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 - 24:	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.