Privacy Impact Assessment (PIA): FDA - GX2 - QTR2 - 2024 - FDA2128954

Created Date: 5/10/2024 12:03 PM Last Updated: 5/23/2024 5:31 PM

Copy PIA (Privacy Impact Assessment)

Do you want to copy this PIA ?

Please select the user, who would be submitting the copied PIA.

Instructions

Review the following steps to complete this questionnaire:

1) Answer questions. Select the appropriate answer to each question. Question specific help text may be available via the icon. If your answer dictates an explanation, a required text box will become available for you to add further information.

2) Add Comments. You may add question specific comments or attach supporting evidence for your answers by clicking on the icon next to each question. Once you have saved the comment, the icon will change to the icon to show that a comment has been added.

3) Change the Status. You may keep the questionnaire in the "In Process" status until you are ready to submit it for review. When you have completed the assessment, change the Submission Status to "Submitted". This will route the assessment to the proper reviewer. Please note that all values list questions must be answered before submitting the questionnaire.

4) Save/Exit the Questionnaire. You may use any of the four buttons at the top and bottom of the screen to save or exit the questionnaire. The button allows you to complete the questionnaire. The button allows you to save your work and close the questionnaire. The button allows you to save your work and remain in the questionnaire. The button closes the questionnaire without saving your work.

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

PIA Name:	FDA - GX2 - QTR2 - 2024 - FDA2128954	**PIA ID:**	1824305
Name of Component:	FDA - OC Cority GX2	**Name of ATO Boundary:**	OC Inventory Control and Information Management System
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	16
Submission Status:	Submitted	**Submit Date:**	5/10/2024
Next Assessment Date:	N/A	**Expiration Date:**	1/1/2100
Office:		**OPDIV:**	FDA
Security Categorization:		**OpDiv PIA ID:**	FDA2128954
Legacy PIA ID:		**Make PIA available to Public?:**	No

1:	Identify the Enterprise Performance Lifecycle Phase of the system.	Operations and Maintenance
2:	Is this a FISMA-Reportable system?	Yes
3:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	Yes
4:	ATO Date or Planned ATO Date.	6/23/2023
5:	Is the system or electronic information collection, agency or contractor operated?	Agency

PTA

PTA

PTA - 2:	Indicate the following reason(s) for this PTA. Choose from the following options.	New
PTA - 2A:	Describe in further detail any changes to the system that have occurred since the last PIA.	
PTA - 3:	Is the data contained in the system owned by the agency or contractor?	Agency
PTA - 4:	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 Office of the Commissioner (OC) Office of Laboratory Safety (OLS) Inventory Control Information Management System (ICIMS) Cority GX2 platform, which encompasses the Occupational Safety and Health Plus (OSH+) application and portal application, Occupational Safety and Health Plus (pOSH +), is to support Agency-wide efforts to improve occupational health, safety, and environmental management. The platform by allowing for real-time reporting and trend analysis. The OLS supports and manages Food and Drug Administration (FDA) wide laboratory science, laboratory security, and environmental, occupational health, and safety operations. The OC OLS ICIMS Cority GX2 platform replaces the OC Safety Inventory Protocol System (SIPS). OSH+ and pOSH+ are web applications tailored from the Commercial Off-The-Shelf (COTS)

product, Cority GX2 (a component of the ICIMS system boundary) to support inventory management, incident investigations, and occupational health details through the base software and its associated modules. OSH+ is the main Cority platform application, which is an enterprise Environmental Health, Safety and Quality (EHSQ) software service that is available to licensed users. The OSH+ application includes the Occupational Health module. Authorized clinicians use PII to retrieve records from this module only. No other module within the OC OLS ICIMS Cority GX2 platform uses PII for retrieval purposes. pOSH+ is the myCority portal platform version that is accessible to non-licensed users and on mobile devices web browser to view the web application.
FDA employees and Direct contractors may use OSH+/pOSH+ to track overall workplace incident reporting, Electronic Health Records (EHRs) and occupational EHRs. Other functionalities include automated notifications generated by pOSH+ to streamline the approval process for incident investigation, alerting each person in the notification chain of the availability of incident safety reports ready for review and resolution. Additionally, pOSH+ enables employees to access their event reports and EHRs, and manage email reminders for appointments, vaccinations, and health surveillance group enrollment and clearance.

OC OLS ICIMS Cority GX2 interfaces with FDA's internal Enterprise Administrative Support Environment (EASE) system (the subject of a separate assessment) via a server link to the ICIMS database. The EASE system

provides a subset of Human Resource (HR) data to ICIMS for use by the Cority GX2 OSH+ and pOSH+ database applications. The ICIMS application server calls the EASE view onto the server. The application server then loads the EASE view using the Human Resource Integration Engine (HRIE) through an Application Programming Interface (API) call. The ICIMS team transfers the employee, and their corresponding organizational/work location tree onto the server and loads this through the Cority Data Integration Engine (CDIE).

The OC OLS ICIMS Cority GX2 applications also interface with FDA Audiometric and Spirometer Engines which use an API call to retrieve data from the Audiometer/Spirometer (FDA medical owned devices) and ingest measurement data into Cority. These devices are used to provide care to individuals. The devices record health condition data (measurement data) for use on care and treatment.

Quest Diagnostics, which is a private third-party laboratory, performs routine tests on blood and tissue samples from FDA clinics. Connectivity to the Quest API (to access laboratory results) is

		configured on the front-end of Cority with a username, password, and an API uniform resource locator (URL). The application server calls the Quest API URL , which ingests any Quest services into Cority GX2. An ICIMS team member can then verify accepted/rejected/updated records on the FDA's Government Furnished Equipment (GFE).
PTA - 5:	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 OC OLS ICIMS Cority GX2 OSH+ and pOSH+ applications maintain data relevant to Occupational Health and Safety. Data captured in the application is used to support workplace incident reporting and EHRs. The system imports the following FDA employee (permanent and Direct Contractors) associated PII from EASE: (a) name; (b) work phone number; (c) medical visit notes; (d) employee identification/patient identification (I.D.) number; (e) date of birth (DOB); (f) medical record identifier; and (g) employment status . The system also collects non-PII: (a) appointments calendar; (b) equipment data; (c) clinic information; (d) inventory; and (e) work center/office location. The OSH+ application includes the Occupational Health module which is used by authorized clinicians to retrieve records. Clinicians use the following PII for this purpose: (a) last name; (b) employee identification/patient identification (I.D.) number; and/or (c) DOB. No other module within the OC OLS ICIMS Cority GX2 platform uses PII for retrieval purposes. FDA employees and Direct Contractors have access to data in the OSH+ and pOSH+ applications as well as administrators. (The developer, Cority Software Inc., does not have access to the data as the data is stored in FDA on-premises servers.)
PTA - 5A:	Are user credentials used to access the system?	Yes
PTA - 5B:	Please identify the type of user credentials used to access the system.	HHS User Credentials HHS/OpDiv PIV Card

PTA - 6:	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 OC OLS ICIMS platform uses the Cority GX2 COTS product to provide the OSH+ and pOSH+ systems. pOSH+ is available to all FDA non-licensed users while OSH+ is limited to license holders. OC OLS ICIMS Cority GX2 is intended to assist OLS with the management of safety and occupational health across the FDA. The FDA uses this system by tracking workplace incidents and the corresponding investigation, and EHRs. OSH+/pOSH+ are internal to the FDA intranet and SSO enabled. The system imports the following FDA employee (permanent and Direct Contractors) associated PII from EASE: (a) name; (b) work phone number; (c) medical visit notes; (d) employee I.D. number/patient I.D.; (e) DOB; (f) medical record identifier; and (g) employment status. The system also collects the following non-PII: (a) appointments calendar; (b) equipment data; (c) clinic information; (d) inventory; (e) work center/office location; and (f) workplace incident review/resolution reports (incident data includes information such as place of incident, if an injury occurred, property damage, conditions, and other information to support an investigation and resolution of the incident). Incident information is captured to aid in improving safety standards with the goal of preventing similar incidents in the future. No PII is captured in these reports. Clinicians use the following PII to retrieve records within the Occupational Health module within OSH+:(a) employee last name; (b) employee ID number; and/or (c) employee DOB. PII data is not used within the full OC OLS ICIMS Cority GX2 platform or other modules in OSH+ or pOSH +.
PTA - 7:	Does the system collect, maintain, use or share PII?	Yes
PTA - 7A:	Does this include Sensitive PII as defined by HHS?	Yes
PTA - 8:	Does the system include a website or online application?	No
PTA - 8A:	Are any of the URLs listed accessible by the general public (to include publicly accessible log in and internet websites/online applications)?	
PTA - 9:	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.	
PTA - 10:	Does the website have a posted privacy notice?	
PTA - 11:	Does the website contain links to non-federal government websites external to HHS?	
PTA - 11A:	Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?	
PTA - 12:	Does the website use web measurement and customization technology?	
PTA - 12A:	Select the type(s) of website measurement and customization technologies in use and if it is used to collect PII.	Session Cookies - Does Not Collect PII
PTA - 13:	Does the website have any information or pages directed at children under the age of thirteen?	
PTA - 13A:	Does the website collect PII from children under the age thirteen?	

PTA - 13B:	Is there a unique privacy policy for the website and does the unique privacy policy address the process for obtaining parental consent if any information is collected?	
PTA - 14:	Does the system have a mobile application?	No
PTA - 14A:	Is the mobile application HHS developed and managed or a third-party application?	
PTA - 15:	Describe the purpose of the mobile application, who has access to it, and how users access it. Please address each element in your response.	
PTA - 16:	Does the mobile application/ have a privacy notice?	
PTA - 17:	Does the mobile application contain links to non-federal government websites external to HHS?	
PTA - 17A:	Is a disclaimer notice provided to users that follow external links to resources not owned or operated by HHS?	
PTA - 18:	Does the mobile application use measurement and customization technology?	
PTA - 18A:	Describe the type(s) of measurement and customization technologies or techniques in use and what information is collected.	
PTA - 19:	Does the mobile application have any information or pages directed at children under the age of thirteen?	
PTA - 19A:	Does the mobile application collect PII from children under the age thirteen?	
PTA - 19B:	Is there a unique privacy policy for the mobile application and does the unique privacy policy address the process for obtaining parental consent if any information is collected?	
PTA - 20:	Is there a third-party website or application (TPWA) associated with the system?	No
PTA - 21:	Does this system use artificial intelligence (AI) tools or technologies?	No

PIA

PIA

PIA - 1:	Indicate the type(s) of personally identifiable information (PII) that the system will collect, maintain, or share.	Name Email Address Phone numbers Medical records (PHI) Date of Birth Mailing Address Medical Records Number Employment Status Patient ID Number
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared.	Employees/ HHS Direct Contractors
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?	FDA uses the PII gathered via OC ICIMS – Cority GX2 (as sourced from FDA EASE, the subject of a separate assessment) for identification purposes related to incident reporting by FDA employees and/or EHRs of FDA employees (identification of individuals involved in work related accidents or those who need to visit the White Oak clinic).
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	The FDA makes no secondary use of the PII.
PIA - 6:	Describe the function of the SSN, Truncated SSN, and/or Taxpayer ID.	
PIA - 6A:	Cite the legal authority to use the SSN, Truncated SSN, and/or Taxpayer ID.	
PIA - 7:	Identify legal authorities governing information use and disclosure specific to the system and program.	Applicable Laws or Regulation Affecting the Systems 5 U.S.C. 301, Departmental Regulations; U.S.C. 7902; Section 19 of the Occupational Safety and Health Act of 1970 (Pub. L. 91-596) as amended (29 U.S.C. 668); Responsibilities for the Maintenance of Records About Individuals by Federal Agencies [OMB Circular A-108, as amended]
PIA - 8:	Are records in the system retrieved by one or more PII data elements?	Yes
PIA - 8A:	Please specify which PII data elements are used to retrieve records.	Employee Last Name, First Name, employee I.D. number/patient I.D., and/or DOB.
PIA - 8B:	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.	SORN 1: OPM GOV-1 General Personnel Records – This SORN only applies to the Occupational Health module within the OSH+ system (only internal to FDA employees). SORN 2: OPM/GOVT 10 Employee Medical File System Records.
PIA - 9:	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains In-person Online Government Sources Other
PIA - 10:	Is there an Office of Management and Budget (OMB) information collection approval number?	No
PIA - 10A:	Provide the information collection approval number.	
PIA - 10B:	Identify the OMB information collection approval number expiration date.	
PIA - 10C:	Explain why an OMB information collection approval number is not required.	An OMB information collection approval number is only required if collecting information from the general public. The OC ICIMS- Cority GX2 application does not collect information from the general public; therefore, an OMB information collection number is not required. The OC ICIMS application only collects information from internal FDA staff.

PIA - 11:	Is the PII shared with other organizations outside the system's Operating Division?	No
PIA - 11A:	Identify with whom the PII is shared or disclosed.	
PIA - 11B:	Please provide the purpose(s) for the disclosures described in PIA - 11A.	
PIA - 11C:	List any agreements in place that authorizes the information sharing or disclosure (e.g., Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or Information Sharing Agreement (ISA)).	
PIA - 11D:	Describe process and procedures for logging/tracking/accounting for the sharing and/or disclosing of PII. If no process or procedures are in place, please explain why not.	
PIA - 12:	Is the submission of PII by individuals voluntary or mandatory?	Voluntary
PIA - 12A:	If PII submission is mandatory, provide the specific legal requirement that requires individuals to provide information or face potential civil or criminal penalties.	
PIA - 13:	Describe the method for notifying individuals that their information will be collected and how they can 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 are no opt-out procedures specific to OC ICIMS – Cority GX2. Employees with operational roles must provide PII to access the system and perform their duties. Individuals who receive care or participate in incident review must also provide their PII to use the system and enable accurate data management.
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.	If FDA changes its practices with regard to the collection or handling of PII related to the system, the Agency will adopt measures to provide any required notice and obtain consent from individuals regarding the collection and/or use of PII. This may include e-mail to individuals, adding or updating online notices, SORNs, Privacy Act Statements, this PIA, relevant forms, or other available means to inform the individual.
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.	Individuals who suspect their PII has been inappropriately obtained, used, or disclosed in any FDA system have many avenues available for assistance. These individuals may contact FDA offices, including the Privacy Office, the Employee Resource and Information Center (ERIC), the FDA Cybersecurity Infrastructure Operations Coordination Center (CIOCC) and other agency offices, via email, phone, and standard mail avenues (all listed on fda.gov and the FDA intranet). All FDA employees and contracts are required to rapidly report any suspected or confirmed security incident and/or data breach to the FDA CIOCC.

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.	Individuals voluntarily provide their PII. The individual is responsible for providing accurate information. Accuracy is ensured by individual review at the time of reporting. FDA personnel may correct/update their information themselves and their PII is relevant and necessary to be granted access to the system. PII relevancy is supported through the design of the system to require and collect only the PII elements necessary to administer the system and enable its intended use. Access is granted and restricted at the individual level as appropriate to the individual's duties (role-based access). Integrity and availability are protected by privacy and security controls selected and implemented while providing the system with an authority to operate (ATO). Controls are selected based on NIST guidance concerning the ATO process, appropriate to the system's level of risk as determined using NIST's Federal Information Processing Standards (FIPS) 199. FDA performs annual reviews to evaluate user access. The agency also reviews the system access list on a quarterly basis to adjust users' access roles and permissions and delete unneeded accounts from the system.
PIA - 17:	Identify who will have access to the PII in the system.	Users Administrators Contractors
PIA - 17A:	Select the type of contractor.	HHS/OpDiv Direct Contractors
PIA - 17B:	Do contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices?	Yes

PIA - 18:	Provide the reason why each of the groups identified in PIA - 17 needs access to PII.	Users can enter and view medical information when creating, reviewing, and completing safety incident reports. A select group of safety and occupational health users, who are granted access via the administrator and receive training, may review medical information (e.g., employee name, injury or illness information) during a medical clinic visit appointment or when providing information about an injury or illness. General users are not permitted to review PII. Administrators can view the demographics module, which displays limited PII information. This module is only turned on when the administrator needs to view information to determine the correct information for medical records. This is rarely turned on and accessed. Contractors, who are maintaining the OC ICIMS – Cority GX2 application and have access to the database, query the PII information to verify that data is correct, and that EASE does not contain data for anyone 13 years of age or younger. Contractors also run other data quality checks and look for orphaned data, which may include PII data from EASE or medical data from the FDA Clinics.
PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	FDA users and Direct Contractors with valid network accounts who require access to the system must obtain supervisory approval and signature before access is granted. The agency reviews the system access list on a quarterly basis to adjust users' access roles and permissions and delete unneeded accounts from the system.
PIA - 20:	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.	The relevant supervisor will indicate on the user account creation form the minimum access that is required for the user to complete his/her job. The scope of access is restricted based on role-based criteria.
PIA - 21:	Identify the general security and privacy awareness training provided to system users (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 system users at FDA take annual mandatory computer security and privacy awareness training. This training includes guidance on Federal laws, policies, and regulations relating to privacy and data confidentiality, integrity, and availability, as well as the handling of data (including any special restrictions on data use and/or disclosure). The FDA Office of Information Management and Technology (OIMT) verifies that individuals successfully complete the training.
PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	Personnel are trained on the use of the system and review HHS Rules of Behavior. Additional role-based training on privacy is available via FDA's privacy office.

PIA - 23:	Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific National Archives and Records Administration (NARA) records retention schedule(s) and include the retention period(s).	PII data is retained in the OC ICIMS – Cority GX2 database for the life of the application. If a request is made to delete an individual's PII data, the OC ICIMS – Cority GX2 Team will delete the information from the application and perform database queries to ensure that the data is no longer present. To date, there have been no requests to delete an individual's PII and no PII has been removed from the application.
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 use of multi-factor access authentication, firewalls, and network monitoring and intrusion detection tools. Physical controls include that all system servers are located at 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 & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	**Privacy Analyst Review Date:**	5/10/2024
Privacy Analyst Comments:		**Privacy Analyst Days Open:**	

SOP Review

SOP Review Status:	Approved	**SOP Signature:**	
SOP Comments:		**SOP Review Date:**	5/10/2024
		SOP Days Open:	0

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	5/23/2024
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte 5/23/2024 Per FDA's Email (see Supporting Documentation), there must be a glitch because the full response doesn't appear in OIS. Noted that on the next iteration of the PIA to cite a NARA approved retention disposition. Other then that this PIA is ready for SAOP review and approval.	**Agency Privacy Analyst Days Open:**	13

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	Signature.docx
SAOP Comments:	Approved on behalf of Bridget Guenther. Please note that the response to PIA-23 is incomplete in the OIS instance and, per FDA, the appropriate records schedules are: **PII data in the OC ICIMS Cority GX2 database is maintained under the following General Records Schedules (GRS):** **(a) GRS 2.7 Occupational Injury and Illness Program Records: Temporary-Destroy when 6 years old, but longer retention authorized if business use requires it.** **(b) GRS 5/6 Item 111 Visitor Processing Records: Temporary-Destroy when 2 years old or longer if business use requires it.**	**SAOP Review Date:**	5/23/2024
		SAOP Days Open:	0

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
5-23-2024_Email_RE FDA - GX2 - QTR2 - 2024 - FDA2128954.msg	219648	.msg	5/23/2024 5:11 PM	0

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 23	BLAND, CRYSTAL	5/23/2024	On the next iteration of the PIA please be sure to cite a NARA Approved retention schedule.	
PIA - 23	BLAND, CRYSTAL	5/23/2024	Per FDA's Email, remaining response: **PII data in the OC ICIMS Cority GX2 database is maintained under the following General Records Schedules (GRS):** **(a) GRS 2.7 Occupational Injury and Illness Program Records: Temporary-Destroy when 6 years old, but longer retention authorized if business use requires it.** **(b) GRS 5/6 Item 111 Visitor Processing Records: Temporary-Destroy when 2 years old or longer if business use requires it.** **Unscheduled deletion of PII in the system may occur in the event of a request by the subject individual. In that event, the OC ICIMS Cority GX2 Team will delete the information from the application and perform database queries to ensure that the data is no longer present. To date, there have been no requests to delete an individual's PII and no PII has been removed from the application.**	

Admin Section

Is OpDiv Privacy Analyst Approved ?:	1	**Is OpDiv Privacy Analyst Return ? :**	0
		Is SOP Return ?:	0
Is Agency Privacy Analyst Approve ?:	1	**Is Agency Privacy Analyst Return ?:**	0
Is SAOP Approved?:	1	**Is SAOP Return ?:**	0
Total Approved:	4	**Total Return:**	0
Total Approval Required:	4		

Miscellaneous Fields

Last Updated:	5/23/2024 5:31 PM	**History Log:**	View History Log