Privacy Impact Assessment (PIA): FDA - Communifire - QTR4 - 2024 - FDA4323855

Created Date: 10/16/2024 12:24 PM Last Updated: 11/13/2024 12:23 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 - Communifire - QTR4 - 2024 - FDA4323855	**PIA ID:**	2324945
Name of Component:	FDA - CDRH Communifire	**Name of ATO Boundary:**	CDRH Center Engagement and Workforce Development
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	28
Submission Status:	Submitted	**Submit Date:**	10/16/2024
Next Assessment Date:	N/A	**Expiration Date:**	1/1/2100
Office:		**OPDIV:**	FDA
Security Categorization:		**OpDiv PIA ID:**	FDA4323855
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?	No
3:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	No
4:	ATO Date or Planned ATO Date.	8/18/2023
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.	PIA Validation (PIA Refresh)
PTA - 2A:	Describe in further detail any changes to the system that have occurred since the last PIA.	Since the last approval of this PTA/PIA, there have been no changes made to this system.
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 Center for Devices and Radiological Health (CDRH) Communifire application is to enhance internal communication and engagement among Center employees. This platform supports the Food and Drug Administration (FDA) and CDRH mission of keeping employees both informed about resources needed to do their work and engaged through internal communications. This system is an internal CDRH-specific implementation of a commercial off-the-shelf (COTS) communications platform/intranet product purchased from an external vendor. Users include authorized CDRH permanent employees and Direct Contractors. These users access the system via a network-level Single Sign-on (SSO) process using multi-factor authentication on their FDA-issued laptops and FDA mobile devices. Through this system, users have access to news, announcements, administrative policies, procedures and other FDA employee-related information and resources. The system is hosted on premises with FDA servers and in FDA data centers. The internal branded name for Communifire is “CDRH-Connect.”
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.	CDRH Communifire collects and maintains the following personally identifiable information (PII) about CDRH permanent employees and Direct Contractors: (a) first and last name; and (b) professional/work e-mail address. This information is imported from FDA’s Active Directory (AD) database (assessed in a separate PIA). CDRH system users also have the option to provide the following PII to their user profiles on a voluntary basis: (a) hire date; (b) profile photo; and (c) work phone number. Users may also opt to provide their work location and division branch to their profiles as well (non-PII which becomes PII when combined with other PII elements). Users may remove this information about themselves at any time. Users of CDRH Communifire can access the following non-PII when using the system: news, announcements, administrative policies, procedures and other FDA employee-related information and resources. PII in the system is not shared with any other system or organization. CDRH maintains information held in Communifire in accordance with applicable records schedules and retention rules. Other than the PII described above, the information accessible to CDRH personnel through Communifire is neither collected by, nor stored in Communifire. The maker of the Communifire system and related mobile application does not have access to any of the PII in the system.

PTA - 5A:	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. The system providing credentials is
PTA - 5B:	Please identify the type of user credentials used to access the system.	
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.	CDRH Communifire is an internal communications platform used only by FDA CDRH permanent employees and Direct Contractors. Its purpose is to provide information, policies, and resources of interest to CDRH employees and to offer a channel for employee engagement. Much of this information has been previously provided by an email newsletter and/or via the inside.FDA intranet. For example, the platform provides centralized navigation and links to already existing information available on other internal FDA sites (FDA-wide intranet). Only CDRH permanent employees and Direct Contractors will consume information offered via CDRH Communifire. CDRH Communifire provides chatting capability within the application. Chats are written conversation displayed as text to the chatting users within the application. Chats are stored in the Communifire database. Users cannot delete these chats via the application. Only authorized database administrators (Admins) may delete chats via direct access to the database. To provide and control user access, the authorized database Admin imports into the Communifire Production database the first and last name, work email address and FDA Center associated with CDRH permanent employees and Direct Contractors. The source of the imported data is the FDA AD system (the subject of a separate assessment). The Communifire application Admin then associates the users with a “Members” group and the system automatically assigns the user an individual profile within the application. CDRH users may choose to add additional PII, if desired, to their individual Communifire profile. User profile information is stored within the database. CDRH does not share any of the PII in the Communifire database with other systems or organizations. Users may access the system only from their Government Furnished Equipment (GFE) using SSO credentials. Access via personal mobile devices is not permitted and is blocked with technical controls (i.e., Communifire equipment sits behind FDA firewalls and there are no external-facing entry or exit points). The version of the application used on FDA mobile devices stores the same data from the same source as the desktop version. Anything that is done in the mobile app will be reflected in the desktop version, and vice versa. There is no third-party software built into Communifire and no data is transmitted to recipients outside CDRH. CDRH does not use Communifire as a data

		repository. The PII and other data stored in Communifire is limited to that which is necessary for the purpose and functionality of the system. Users may search the system using any terms. However, a user search is not a search of the data in the system, rather it is a search across other pre-existing sources of available information internal to the FDA. Content of those source systems and accessibility is controlled by the managers of the source systems; restricted information is not made available to Communifire users.
PTA - 7:	Does the system collect, maintain, use or share PII?	Yes
PTA - 7A:	Does this include Sensitive PII as defined by HHS?	No
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.	
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?	Yes
PTA - 14A:	Is the mobile application HHS developed and managed or a third-party application?	HHS
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.	The purpose of the mobile application is to provide authorized users (FDA CDRH employees and Direct Contractors) with the ability to access FDA sponsored content when using their GF mobile devices. Users access the mobile application by using the following URL: https://cdrhhome.fda.gov.
PTA - 16:	Does the mobile application/ have a privacy notice?	No
PTA - 17:	Does the mobile application contain links to non-federal government websites external to HHS?	No
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?	No

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?	No
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 Photographic Identifiers Mailing Address
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?	CDRH employees use PII to establish their user profile in the system.
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.	Federal Food, Drug and Cosmetic Act (FD&C Act) United States Code, Title 21; 5 U.S.C. 301.
PIA - 8:	Are records in the system retrieved by one or more PII data elements?	No
PIA - 8A:	Please specify which PII data elements are used to retrieve records.	
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.	
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
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.	CDRH Communifire does not collect information from any persons other than federal employees and Direct Contractors serving in their official capacities and therefore does not require an OMB information collection approval number.
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.	CDRH staff have the option not to use Communifire. Employee information required for the performance of duties is available through other means and channels within FDA. Otherwise, FDA permanent employees and Direct Contractors must provide their PII for authentication to FDA systems. There is no option for individuals to opt-out regarding the collection of their PII data. If an FDA permanent employee or Direct Contractor chooses not to provide PII, this would result in non-hire and inability to access or login to the FDA network or access Communifire.
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 regarding the collection or handling of PII related to Communifire, the Agency will implement 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, 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.	If CDRH employees have questions or concerns about their information in the system, they may contact the Employee Resource and Information Center (ERIC), send an email to a designated e-mail address for use by information senders, or click a “help” icon within the application. The information sender e-mail account is a shared email box that the Communifire owner monitors. Employees with concerns about inaccuracy, misuse or disclosure of information about them have multiple additional avenues available to obtain assistance, including: their supervisors, a 24-hour FDA technical assistance line, FDA's Cybersecurity Infrastructure Operations Coordination Center (CIOCC), and the FDA Privacy Office. Under federal, HHS and FDA policy, all permanent employees, Direct Contractors and other individuals performing services for or on behalf of FDA must rapidly report all known or suspected incidents and data breaches to 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 most of the PII in the system, other than their name and CDRH Office information. The individual is responsible for providing accurate information. Accuracy is ensured by individual review if they choose to enter it. FDA personnel may correct/update their information themselves at any time. Beyond their name and office information, users decide if their PII is relevant and necessary to be entered into the system. The CDRH system and application administrators perform weekly reviews of users to evaluate and remove or adjust access. Data discrepancies identified during system use are addressed when discovered.
PIA - 17:	Identify who will have access to the PII in the system.	Users Administrators Developers 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-All users will have an employee profile that contains their name. Each person's profile is accessible to others in the system. Administrators-Require access for system maintenance and administrative purposes. Developers-For development and support purposes. Contractors-Some of the users are Direct Contractors.
PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	CDRH leadership and application admins determined that only CDRH employees and Direct Contractors are allowed to access Communifire (and thus see PII held in the system). The system and application admins review the user list on at least a weekly basis. The system/application admins ban and/or delete any non-CDRH users that access the URL and notify them via email that the system is for CDRH employees only. Banning is a function within Communifire, and it prevents users from accessing the site. The site will refuse to connect, and the user will see an error in their browser. The user won't see a message regarding their account status.
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.	Only CDRH permanent employees and Direct Contractors have access to the PII that is available in users' profiles within Communifire. Access to this contact information is necessary for the effective use of the system to share knowledge across CDRH. The URL is not available to anyone outside of FDA. If a non-CDRH user attempts to access the system, the system/application administrators ban and/or delete them and notify them via email that the system is for CDRH employees only. Banning is a function within Communifire, and it prevents users from accessing the site. The site will refuse to connect, and the user will see an error in their browser. The user won't see a message regarding their account status.
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 Digital Transformation (ODT) verifies that training has been successfully completed. System Administrators must further complete the HHS Information Security for IT Administrator training before given privileged access.

PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	Administrators receive training about implementation of Communifire provided by the maker of Communifire software, Axero. Users who are not administrators will receive basic training about how to access and navigate the system.
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).	The applicable records retention schedules are: FDA-9480b, GRS 5.2 Item 010, Transitory records. Temporary. Destroy when no longer needed for business use, or according to agency predetermined time period or business rule. FDA-8400 General Program Files. Includes files relating to FDA programmatic activities. They may relate to Program subject files and routine program management files that are not covered elsewhere in the FDA Records Control Schedules. FDA-8200 Calendars, Schedules and Logs of Daily Activities. Files relate to calendars, schedules, logs, appointment books, diaries and other records documenting meetings, appointments, telephone calls, trips, visits and other activities of Federal employees while serving in an official capacity, excluding materials determined to be personal.
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.	Technical Safeguards include use of multi-factor access authentication, firewalls, and network monitoring and intrusion detection tools. Users must be FDA/CDRH permanent employees and Direct Contractors who already have authorized Personal Identity Verification card (PIV) access to the FDA network and are using FDA government furnished equipment. Non-CDRH users are banned from the site. Although the process of banning is manual, system and application administrators conduct their reviews on at least a weekly basis. For physical controls, all related servers are located within authorized FDA data center facilities and are protected by guards, locked facility doors, and climate controls. Servers are configured to be monitored by Office of Information Management & Technology (OIMT) network and database monitoring software to detect anomalies. Administrative safeguards include user training; system documentation that advises on proper use; PII stored in the system is kept to a minimum as it is needed to identify system users. The remaining PII is voluntarily provided, if desired, and the user may remove it at any time. 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:**	10/16/2024
Privacy Analyst Comments:		**Privacy Analyst Days Open:**	

SOP Review

SOP Review Status:	Approved	**SOP Signature:**	
SOP 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.	**SOP Review Date:**	10/16/2024
		SOP Days Open:	0

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	10/24/2024
Agency Privacy Analyst Review Comments:	Reviewer: Shanai Shobowale 10/24/2024 This PIA is ready for SAOP review and approval.	**Agency Privacy Analyst Days Open:**	8

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	Archer Signature_Bridget Guenther.docx
SAOP Comments:	Per FDA, The PIA is currently experiencing an Archer error with Question #3 of the general information. Q-3 "Does the system have or is it covered by a Security Authorization to Operate (ATO)? The FDA instance of Archer is reflecting "No" as the answer when the correct answer is "Yes." The FDA Archer Team is aware of this occurrence and is working on a solution.	**SAOP Review Date:**	11/13/2024
		SAOP Days Open:	20

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
CDRH Communifire_SOP Approved.rtf	761800	.rtf	10/17/2024 8:35 AM	0

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 1	BLAND, CRYSTAL	10/24/2024	Per FDA, The PIA is currently experiencing an Archer error with Question #3 of the general information. Q-3 “Does the system have or is it covered by a Security Authorization to Operate (ATO)? The FDA instance of Archer is reflecting “No” as the answer when the correct answer is “Yes.” The FDA Archer Team is aware of this occurrence and is working on a solution.	

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:	11/13/2024 12:23 PM	**History Log:**	View History Log