Privacy Impact Assessment (PIA): FDA - GovDelivery - QTR4 - 2024 - FDA4563414

Created Date: 10/22/2024 4:26 PM Last Updated: 11/13/2024 1:38 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 - GovDelivery - QTR4 - 2024 - FDA4563414	**PIA ID:**	2350972
Name of Component:	FDA - OC GovDelivery	**Name of ATO Boundary:**	OC GovDelivery
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	22
Submission Status:	Submitted	**Submit Date:**	10/22/2024
Next Assessment Date:	N/A	**Expiration Date:**	11/13/2027
Office:		**OPDIV:**	FDA
Security Categorization:		**OpDiv PIA ID:**	FDA4563414
Legacy PIA ID:		**Make PIA available to Public?:**	Yes

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)?	No
4:	ATO Date or Planned ATO Date.	9/5/2023
5:	Is the system or electronic information collection, agency or contractor operated?	Contractor

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?	Both

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 Food and Drug Administration (FDA) Office of the Commissioner (OC) GovDelivery Communications Cloud (GovDelivery) is a web-based email subscription management application, provided by Granicus, a Software as a Service (SaaS), commercial-off-the-shelf (COTS) product, that allows members of the general public to subscribe to get information from the FDA via email and potentially via text message. FDA uses the GovDelivery service to deliver bulletin messages to self-subscribed users. The GovDelivery user selects specific topics that interest them. The purpose(s) of FDA's use of GovDelivery is to provide individuals an opportunity to use GovDelivery to subscribe to receive regular e-mails with information about regulated foods, drugs, cosmetics, tobacco, veterinary medicines, and other health and regulatory information relevant to the FDA. Internal system users, referred to as Topic Administrators, will use the system to disseminate public information relating to FDA and its programs and services.
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.	Any individual with internet access may establish an account with GovDelivery and use it to subscribe to email and text messaging delivery of information about the FDA. GovDelivery users include FDA personnel (permanent employees and Direct Contractors) and members of the public. Users voluntarily provide their name, e-mail address and/or phone number (also referred to as contact information) directly to GovDelivery in order to receive information through GovDelivery. Phone numbers are collected only for those who voluntarily opt in to receive SMS notifications. GovDelivery maintains these e-mail addresses and phone numbers. They may also be made available to FDA, but FDA does not collect or maintain user contact information within the FDA environment. In addition to email subscriptions, GovDelivery also has a specific texting (short message service, SMS) functionality, that individuals may choose to use. GovDelivery collects phone numbers of those who voluntarily opt in to receive SMS notifications. The SMS function provides members of the public an option to self-subscribe for SMS via a web link or Quick Response (QR) code. The SMS function also offers the unsubscribe capability. FDA does not collect or maintain any personally identifiable information (PII) about GovDelivery users, including both members of the public and FDA personnel. User contact information collected by GovDelivery is necessarily used by GovDelivery to enable requestors to receive information from the FDA electronically via e-mail or text. GovDelivery maintains this contact information for the duration the platform is in use.

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 PII about individuals that is collected consists of user contact information (name, email address, phone number) and user topic preferences. Phone numbers are collected only for those who voluntarily opt in to receive SMS notifications. This information is necessary and is used for providing information in response to a user's requests and administering user accounts. GovDelivery allows a member of the public (user) to subscribe to news and information on FDA websites. The GovDelivery user selects specific topics that interest them. Whenever information on that topic is made available by the Agency, the user that has subscribed to that topic receives a message (email or text SMS). The user's subscription profile consists of their email address and the topics they wish to receive email updates for. The user may customize and manage their subscription profile in order to receive exactly the types of information they desire, and they may cancel their subscriptions at any time. Subscribers can choose from numerous subscriptions offered by the FDA, including, but not limited to: Press releases; Newsletters; Product and Device Recalls; Updated Guidelines; and other Public Health related topics. The Agency also uses GovDelivery for internal email communications with FDA staff (for instance, to invite staff to events). Users can subscribe, via a secure Web page, to receive FDA emails through various signup pages on FDA website properties, including: www.FDA.gov; and https://public.govdelivery.com/accounts/USFDA/subscriber/new. The FDA Office of External Affairs (OEA), Web and Digital Services Staff serves as the executive agent for the FDA GovDelivery Service and controls who at the Agency has access to send email bulletins and create or delete topics. Only select authorized FDA employees on this team have access to the system at an Administrator level role. Account Administrators (Admins) can create topics and delete topics, access all subscriber information, security reports, and account metrics. Other high-level functions include determining if a topic list is public facing or non-public facing. In addition, Account Admins have access to all user and subscription information in the system. Internal system users include FDA Employees and Direct Contractors. These users can access the system at a Topic Level role. Topic Admins, have basic level access which include, sending and

		creating bulletins, creating templates, and maintaining topic lists, and viewing reports. Topic Admins only have access to the topics that they are assigned access to. Account Admins and Topic Admins access GovDelivery through the web: https://admin.govdelivery.com/ . Login credentials are provided to internal FDA users, to include account Admins and Topic Admins, through Max.gov to enable PIV card access. Only FDA employee users with an FDA issued PIV card can access the OC GovDelivery system. The GovDelivery System Developers have access to the platform for the purpose of troubleshooting and system maintenance but cannot access the OC GovDelivery system through the web sign-on because our sign-on is PIV Card protected. FDA uses the contact information provided by users only to send messages to the specific user related to the topics selected by the user in the GovDelivery system. FDA will not use the GovDelivery service or associated information for any other purposes. FDA will not send messages not related to the topics selected by the user and will not actively seek additional PII from individuals.
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?	Yes
PTA - 8A:	Are any of the URLs listed accessible by the general public (to include publicly accessible log in and internet websites/online applications)?	Yes

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.	The purpose of the website is to provide individuals with an email subscription service to subscribe to receive regular e-mails with information about regulated foods, drugs, cosmetics, tobacco, veterinary medicines, and other health and regulatory information relevant to the FDA. Users (public) can subscribe, via a secure Web page, to receive FDA emails through various signup pages on FDA website properties, including: • www.FDA.gov • https://public.govdelivery.com/accounts/USFDA/subscriber/new The FDA Office of External Affairs (OEA), Web and Digital Services Staff serves as the executive agent for the FDA GovDelivery Service and controls who at the Agency has access to send email bulletins, create or delete topics. Only select agency staff from this team have access to the system at an Admin level role. Account Admins have access to all user and subscription information in the system. Internal users of the system (FDA Employees and Direct Contractors) can access the system at a Topic Level role. Topic Admins have basic level access which include, sending and creating bulletins, creating templates, and maintaining topic lists, and viewing reports. Topic Admins only have access to the topics that they are assigned access to. Both the Account Admin and Topic Admins access GovDelivery through the web: https://admin.govdelivery.com/ . Login credentials are provided through Max.gov to enable PIV card access. No user without an FDA issued PIV card can access the internal system. The GovDelivery System Developers have access to the platform for the purpose of troubleshooting and system maintenance but cannot access our system through the web sign on because our sign on is PIV card protected.
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?	Yes
PTA - 11A:	Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?	Yes
PTA - 12:	Does the website use web measurement and customization technology?	No
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?	No
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?	Yes
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
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared.	Employees/ HHS Direct Contractors Members of the public
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?	The FDA uses the PII for the primary purpose of disseminating email information for subscribers who have voluntarily opted in to receive information from FDA and its programs and centers. Other opted include agency stake holders. PII is in the form of name, email addresses and/or phone number. Email addresses are collected through a subscription sign up page. Some of the email addresses have been transferred and uploaded from FDA's previous email distribution software. Other contacts have been uploaded or transferred from center-maintained email lists. Phone number is used to address user requests to receive information via SMS text.

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.	5 U.S.C. 301 which provides authority for the agency to establish the organizations, procedures and tools necessary to perform its duties and pursue its mission. Information use and disclosure for this system is governed by the laws and regulations of the individual business practice that this system is used to conduct. Users work in various agency organizations that have different functions and are subject to different laws and regulations.
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 Other HHS OPDIV State/Local/Tribal Other Federal Entities Non-Government Sources Members of the Public
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.	The collection of mailing addresses, email addresses, or mobile numbers for newsletters, text alerts, agency updates, and other publications are not subject to Paperwork Reduction Act (PRA) requirements and an OMB collection approval number is not required.
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.	Users may opt not to use FDA GovDelivery and never provide their PII to the FDA. It is not possible to use GovDelivery to receive email or text messages without providing this PII. Users may find similar information on FDA.gov without providing any PII and may also self-subscribe to FDA email lists outside of the GovDelivery platform and thereby avoid providing their PII to GovDelivery.
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 the collection, use, or sharing of PII data in the system, FDA will notify affected individuals by the most efficient and effective means available and appropriate to the specific change(s). For example, sending an e-mail notice to the individuals to provide notice and a means of providing any required consent. Other actions could include updating this PIA and including notice in other communications and on FDA.gov.
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 several options available to them to resolve the situation. These individuals may contact FDA offices via email, phone and standard mail avenues (all listed on fda.gov). This includes the FDA Privacy Office, FDA's GovDelivery Account Administrator, and FDA's Cybersecurity and Infrastructure Operations Coordinating Center (CIOCC). In addition, individuals can also self-unsubscribe from any FDA GovDelivery account. Because GovDelivery software is used for email marketing and distribution, FDA is required by law to provide a means to unsubscribe from unwanted communication. All permanent and contract employees are required to rapidly report any suspected breaches to the 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.	In conjunction with the quarterly User Access Review, FDA reviews Admin accounts. Accounts are removed for users who no longer require access to the system. Once removed from the systems, the Admins no longer have access to PII data. PII is provided voluntarily by the individual. The individual is responsible for providing accurate information (email or phone number). GovDelivery's system is equipped to recognize false, inaccurate or bot email addresses. Once an email address is deemed undeliverable, the system will automatically delete the email. FDA personnel may also correct/update their information themselves and their PII is relevant and necessary to be granted access to the system. Relevancy is ensured by technical and process design to collect and process only PII as necessary for system purposes. 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 in the course of providing the system with an authority to operate (ATO). Controls are selected based on National Institute of Standards and Technology (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. GovDelivery is FedRAMP approved and leverages National Institute of Standards and Technology (NIST) standards and guidelines to provide standardized security requirements for cloud services; a conformity assessment program; standardized authorization packages and contract language; and a repository for authorization packages.
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/Subscribers: Will have access to their own PII, and employees will have access to the PII about their subscription choices, email addresses and phone numbers. Administrators: Will have access to user PII when needed for GovDelivery administrative tasks. Developers: Will have access to user PII for system development, implementation, and operations and maintenance tasks. Contractors: Direct contractors are contractors that work for HHS/FDA and deemed necessary for their role, will have the same access as users.
PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Access to PII in the system is granted and restricted at the individual level as appropriate to the individual's duties (role-based access). Admins must review and approve requests for access to PII about individuals other than the individual seeking access. Individual's whose role does not require access to PII about other users are not given that access.
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.	Role based access controls (RBAC) including Admin controlled technical settings are employed to ensure that users have only the necessary access to perform their job duties. Management establishes roles for individual personnel, with the technical controls applied to enforce role-based restrictions permitting access only to information that is required for each individual to perform his/her job.
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 FDA system users complete annual FDA information security and privacy awareness training that specifically addresses privacy topics.
PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	Internal system users are provided with a user guide and live training and guidance.
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 not retained by the FDA GovDelivery account (system). Separately, GovDelivery maintains user contact information, not the FDA. GovDelivery maintains information for six years after a user submits an unsubscribe request.

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. FedRAMP security safeguards are in place to provide cloud security and protection. Other appropriate controls have been selected from the 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:**	10/22/2024
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:**	10/22/2024
		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: Nestor Villafuerte 10/24/2024 All comments have been addressed, this PIA is ready for SAOP review and approval.	**Agency Privacy Analyst Days Open:**	2

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	Archer Signature_Bridget Guenther.docx
SAOP Comments:		**SAOP Review Date:**	11/13/2024
		SAOP Days Open:	20

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
10-24-2024 EMAIL_PIAs in Queue (OC GovDelivery).pdf	387156	.pdf	10/24/2024 10:11 AM	0
OC GovDelivery_SOP Approved.pdf	178549	.pdf	10/23/2024 9:59 AM	0

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 1	VILLAFUERTE, NESTOR	10/23/2024	On the next iteration of the PTA, please remove any bullet points for 508 compliance. Reviewer notes that the ATO date posted has passed, and the response to an active ATO is marked "No". Please confirm.	

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 1:38 PM	**History Log:**	View History Log