Privacy Impact Assessment (PIA): FDA - GUDID - QTR4 - 2023 - FDA2125076

Created Date: 12/22/2023 3:02 PM Last Updated: 1/4/2024 3:46 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 - GUDID - QTR4 - 2023 - FDA2125076	**PIA ID:**	1748411
Name of Component:	FDA - CDRH Global Unique Device Identifier Database	**Name of ATO Boundary:**	CDRH Regulatory Review
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	13
Submission Status:	Submitted	**Submit Date:**	12/22/2023
Next Assessment Date:	N/A	**Expiration Date:**	1/3/2027
Office:		**OPDIV:**	FDA
Security Categorization:		**OpDiv PIA ID:**	FDA2125076
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?	No
3:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	Yes
4:	ATO Date or Planned ATO Date.	10/11/2022
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.	No privacy related changes have occurred since the last Privacy Impact Assessment (PIA) was completed.
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 Center for Devices and Radiological Health (CDRH) Global Unique Device Identification Database (GUDID) system serves as the definitive source for device identification information for medical devices used in the United States. The GUDID system provides the means for device labeling organizations to submit, store, and access device identifiers and associated product data for all medical devices. Users of the CDRH GUDID system will include Food and Drug Administration (FDA) employees and Direct Contractors, healthcare providers, and the general public. Healthcare providers and the general public will access the system via AccessGUDID, a web site hosted by the National Library of Medicine (NLM).

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.	Section 226 of the FDA Amendments Act (FDAAA) of 2007 and Section 614 of the FDA Safety and Innovation Act (FDASIA) of 2012 amended the Federal Food, Drug, and Cosmetic Act to add section 519(f), directing the FDA to promulgate regulations establishing a unique device identification system for medical devices. In meeting this objective, the CDRH GUDID system allows device labeling organizations to submit device identification information one record at a time via the GUDID Web Interface or as an Extensible Markup Language (xml) file via the FDA Electronic Submission Gateway (ESG, subject of a separate assessment). The system allows labeling organizations to update and add additional information as necessary. The system is designed to improve medical device safety by providing users with a publicly available database that contains a consistent stream of unambiguous and up-to-date device product information. The system collects externally sourced personally identifiable information (PII) from data submitters and regulatory contacts. Contact information is collected to establish an account, to support public access to device information, and for communication purposes by and between the FDA and data submitters and regulatory contacts (to include patients and consumers seeking answers to device related questions). The GUDID system collects and maintains the following PII: (a) name; (b) work email address; (c) work telephone number; and (d) username and password. Additionally, device identification information that can be released to the public is made available via AccessGUDID, hosted by NLM. The device identifiers maintained in the system are not linkable to individuals.
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.	

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 CDRH GUDID system allows device labeling organizations to submit device identification information one record at a time via the GUDID Web Interface or as an Extensible Markup Language (xml) file via the FDA ESG, (subject of a separate assessment). Users of the system can also update and add additional information when necessary. PII collected is (a) name; (b) work email address; (c) work telephone number; and (d) username and password. The regulatory contact information stored in the GUDID system for a device manufacturer is used only by authorized FDA users for any device data clarifications. The support contact work email address and work telephone numbers are used by the public users for help-desk support. In most cases this information will refer to a role or office, not an individual, and will not be PII. The employee information is used for account management and access.
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 publicly accessible GUDID website is the portal through which external users access the application and submit device identification related data. User access requires a username and password.
PTA - 10:	Does the website have a posted privacy notice?	Yes
PTA - 11:	Does the website contain links to non-federal government websites external to HHS?	No
PTA - 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?	Yes
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?	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?	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 User Credentials Other - Free text Field - All contact information collected is professional/work contact information.
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared.	Employees/ HHS Direct Contractors Patients 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 regulatory contact information stored in the GUDID system for a device manufacturer is used by FDA authorized users only for any device data clarifications. The support contact work email address and work telephone numbers are used by the public users for help-desk support. In most cases this information will refer to a role or office, not an individual, and will not be PII. The employee information is used for account management and access.

PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	The FDA does not make any secondary uses of the PII collected.
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.	The Federal Food, Drug, and Cosmetic Act, section 519(f)-Use of usernames and passwords are required by the Federal Information Security Modernization Act (FISMA) and guidance issued pursuant to that Act.
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 Email Online Government Sources Within the OPDIV Non-Government Sources Private Sector
PIA - 10:	Is there an Office of Management and Budget (OMB) information collection approval number?	Yes
PIA - 10A:	Provide the information collection approval number.	The OMB information collection approval number is 0910-0485.
PIA - 10B:	Identify the OMB information collection approval number expiration date.	3/31/2026
PIA - 10C:	Explain why an OMB information collection approval number is not required.	N/A
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.	The collection of PII is “voluntary” as that term is used by the Privacy Act, but regulated entities are required to submit contact information for FDA to conduct communications and oversight with regulated entities. GUDID does not provide an opt-out process. The contact information is required for access to the system and for FDA purposes if questions arise.
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.	No changes affecting individuals’ privacy rights or interests are expected, if there were to be such changes FDA would notify individuals using the contact information they have provided, notices on FDA web sites, or other appropriate means.
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.	GUDID leverages a help-desk to provide an avenue by which all users of the system can submit questions and concerns and receive responses. Additionally, individuals may contact the FDA’s Privacy Office for assistance. FDA employees and Direct Contractors may also contact their Information System Security Officer (ISSO), or FDA’s Employee Resources and Information Center (ERIC) to seek assistance with any PII use or disclosure concerns or to correct inaccurate information. Also, individuals may report such concerns to the Cybersecurity and Infrastructure Operations Coordination Center (CIOCC) via email, telephone, and standard mail (all listed on fda.gov and the FDA intranet). In the event of a suspected incident or data breach of PII, all FDA personnel and Direct Contractors are required to report that without delay to the FDA’s CIOCC who will notify the Privacy Office.
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.	Regulated entities are responsible for providing timely, complete and accurate POC information. Integrity and availability are protected by security controls selected as appropriate for the system's level of risk and consistently with guidance from the National Institutes of Standards and Technology (NIST). Because the PII is administrative in nature (not used to determine or issue benefits, etc.) and is the responsibility of the submitter FDA does not conduct periodic reviews of the PII (work contact information). CDRH periodically reviews FDA user account information, and inaccurate or outdated information is corrected. External entities are responsible for providing FDA with current information, such that external Coordinator accounts and external users accounts may be updated if necessary.
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 will have access to their own data; external Coordinators (one per labeling organization) will have access to the data of all users at their facility. FDA administrators will have access to all contact information for purposes of contacting users at labeling organizations and verifying submitted data. Developers will have access to all data as part of development purposes (troubleshooting, system maintenance). Developers and Data Base Administrators (DBAs) are Direct Contractors.
PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	The agency uses enterprise-wide controls. Procedures include separation of duties between system managers, change control personnel, users, and developers; access to the application at any level must first be reviewed and approved by management.
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.	Access approvals are implemented via technical permission settings. Submitters will only have access to their own data. Coordinators have access only to data from their own companies. The only other users with access to PII would be developers and DBAs, and access would only be required when modifying or further developing the system. Individuals in these roles would only be authorized to access PII as needed to accomplish the specific tasks they have been assigned.
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.
PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	System users are not provided additional training. External industry users are not provided security and privacy training as they should not have access to any privacy information other than the information they submit themselves, although there is also a system user agreement warning banner on the main login page. By clicking on the login, they are agreeing to the system user statement, which includes privacy and security warnings.

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).	For the contact information PII in the system, the current retention schedule is FDA File Code 7222, Database Records, National Archives and Records Administration (NARA) Approval N1-88-07-2. Retention is temporary, with cutoff after the establishment goes out of business or the product is no longer commercially marketed, and the records would be deleted or destroyed after ten years after cutoff or when no longer needed for legal, research, historical or reference purposes, whichever is the latest. System account credentials remain available as long as each user has authorized access to the system. Credentials are revoked when access is no longer needed, including if the individual moves to a different office within FDA or leaves FDA employment. These records are maintained under the new General Records Schedule (GRS) FDA 9962-GRS 3.2, Item 030-System Access Records. Systems not requiring special accountability for access. GRS-2013-0006-0003), which is for “records … created as part of the user identification and authorization process to gain access to systems. " Under this schedule, retention is until "business use ceases." In other words, NARA concurs that agencies may dispose of these records as soon as they are no longer needed.
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:**	12/22/2023
Privacy Analyst Comments:		**Privacy Analyst Days Open:**	

SOP Review

SOP Review Status:	Approved	**SOP Signature:**	
SOP Comments:		**SOP Review Date:**	12/22/2023
		SOP Days Open:	0

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	1/2/2024
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte This PIA is ready for SAOP review and approval.	**Agency Privacy Analyst Days Open:**	11

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	Archer Signature_Bridget Guenther.docx
SAOP Comments:		**SAOP Review Date:**	1/4/2024
		SAOP Days Open:	2

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
No Records Found				

Comments

Question Name	Submitter	Date	Comment	Attachment
No Records Found				

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:	1/4/2024 3:46 PM	**History Log:**	View History Log