US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

10/06/2016

OPDIV:

FDA

Name:

Global Unique Device Identifier Database

PIA Unique Identifier:

P-8780769-332067

The subject of this PIA is which of the following?

Major Application

Identify the Enterprise Performance Lifecycle Phase of the system.

Operations and Maintenance

Is this a FISMA-Reportable system?

Yes

Does the system include a Website or online application available to and for the use of the general public?

Yes

Identify the operator.

Agency

Is this a new or existing system?

Existing

Does the system have Security Authorization (SA)?

No

Indicate the following reason(s) for updating this PIA.

PIA Validation

Not applicable. This is a new in-development system and new PIA.

Describe in further detail any changes to the system that have occurred since the last PIA.

Members of the public can now download some of the information stored in GUDID through AccessGUDID, a web site hosted by the National Library of Medicine at the National Institutes of Health.

Describe the purpose of the system.

The 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. The GUDID will also be accessible by healthcare providers and the general public via AccessGUDID, a web site hosted by the National Library of Medicine.

Describe the type of information the system will collect, maintain (store), or share.

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. The FDA published a Final Rule establishing Unique Device Identifier (UDI) regulations on September 24, 2013. The creation of a Global Unique Device Identifier Database (GUDID) system aims to improve medical device safety by providing a publicly available database that facilitates access by patients, care providers and other members of the public to information about medical devices, including the device identifiers. The GUDID system is intended to improve medical device safety by providing a public, standard data source of consistent, unambiguous device product information. In order to meet this objective, device labeling organizations are required to provide device identification information, including the device identifier, and associated administrative data. Device labeling organizations may be the manufacturers of the devices, or they may be other kinds of businesses such as distributors.

The only externally sourced PII collected in the GUDID system is contact information for data submitters and regulatory contacts at the labeling organization. This includes their work e-mail address, name, and work telephone number. Contact information is collected to establish an account, to support public access to device information, for purposes of communication in the event FDA needs additional information, and/or FDA verification of submitted data.

The system collects and maintains username and passwords for both internal FDA users and external industry users. System Administrators establish usernames and temporary password for the internal FDA users and external Coordinators. External Coordinators may create additional accounts for additional industry users. Coordinators and other industry users have access to information about their own organizations only. Users are not able to change the user name after it is established.

Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.

The 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 collects contact information for data submitters and regulatory contacts. This will include their name, work e-mail address, and work telephone number.

In addition to FDA's use of the information as described in this assessment, phone number and e-mail address for points of contact is expected to be used by patients and consumers seeking answers to device-related questions.

Additionally, device identification information that can be released to the public is made available via AccessGUDID, hosted by National Library of Medicine (NLM). The device identifiers maintained in the system are not linkable to individuals.

Does the system collect, maintain, use or share PII?

Yes

Indicate the type of PII that the system will collect or maintain.

Name

E-Mail Address

Phone Numbers

E-mail address, mailing address, name, and phone number above refer to work contact information for data submitters, e.g., the point of contact at a device manufacturer .
E-mail address, name, and phone number above refer to work contact information for system users (internal and external), data submitters and regulatory contacts, e.g., the point of contact at a device manufacturer.
Note: Device identifiers maintained in the system are not linkable to individuals.

Logon information is also present in the system (username and password).

Indicate the categories of individuals about whom PII is collected, maintained or shared.

Employees

Public Citizens

Public Citizen refers to a device labeling organization's regulatory point of contact (name, work e-mail address, work phone number), to whom the FDA should address correspondence, and the labeling organization's designated support point of contact, which is the person or organization that members of the public may contact with questions or concerns. For the support point of contact, work e-mail address and work phone number are supplied; name is not collected or released, and the support point of contact information may represent a role or office rather than an individual and will therefore most often not constitute PII.

Employee information is collected for user access only.

How many individuals' PII is in the system?

500-4,999

For what primary purpose is the PII used?

The regulatory contact information stored in the GUDID for a device manufacturer is used by FDA (only) for any device data clarifications.

The support contact work e-mail address and work phone 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.

Describe the secondary uses for which the PII will be used.

None.

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 Management Act and guidance issued pursuant to that Act.

Are records on the system retrieved by one or more PII data elements?

No

Not applicable.

Identify the sources of PII in the system.

Online

Other

Government Sources

Within OpDiv

Identify the OMB information collection approval number and expiration date

OMB Control 0910-0720 expires December 31, 2016.

Is the PII shared with other organizations?

No

Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.

The GUDID Guidance document prepared by FDA provides entities and individuals who submit information background about the different user roles in GUDID and the need for the type of information collected in the GUDID.

Additionally, during the GUDID Account Request process, users are notified that their user information is not made available to the public. Support POC information is made available to the public, but typically refers to an office or role and does not constitute PII.

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.

Is the submission of PII by individuals voluntary or mandatory?

Voluntary

Describe the method for individuals to opt-out of the collection or use of their PII. If there is no option to object to the information collection, provide a reason.

The collection of PII is “voluntary” as that term is used by the Privacy Act, but regulated entities are required to submit contact information in order 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.

Process to notify and obtain consent from individuals whose PII is in the system when major changes occur to the system.

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.

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.

GUDID leverages a help desk to provide an avenue by which users can submit questions and concerns and receive responses. Additionally, in the event of a suspected privacy breach or security incident, the FDA maintains an agency process which all employees must follow.

Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy.

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. 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.

Identify who will have access to the PII in the system and the reason why they require access.

Users:

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.

Administrators:

FDA administrators will have access to all contact information for purposes of contacting users at labeling organizations and verifying submitted data.

Developers:

Database administrators will have access to all data as a routine part of their job.

Contractors:

Developers and DBAs are direct contractors.

Describe the 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.

Describe the 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 database administrators, 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.

Identify training and awareness provided to personnel (system owners, managers, operators, contractors and/or program managers) using the system to make them aware of their responsibilities for protecting the information being collected and maintained.

All personnel are required to complete FDA's online security and privacy awareness training at least once a year.

Describe 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.

Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?

Yes

Describe the process and guidelines in place with regard to the retention and destruction of PII.

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 FDA File Code 9962 (NARA GRS 20, Item 1c; superseded by the new GRS 3.2, item 030 (DAA-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.

Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.

Information contained within this system is protected by several layers of administrative, physical, and technical controls in accordance with policies and regulations from the FDA, National Institute of Standards and Technology, and Office of Management and Budget. All applicable security controls are reviewed on a periodic basis to ensure that they are implemented correctly, operating as intended, and producing the desired result of protecting all information. The administrative controls include annual security and privacy training and Rules of Behavior required of all FDA Employees and direct contractors, which includes adhering to the policies and procedures governing security breaches and reporting requirements. External users are not provided the FDA mandated training, but do not have access to any information other than the information they provide themselves. Technical controls include secured access (e.g., user name and passwords) and are captured in the GUDID System Security Plan and associated Authority to Operate documentation. Physical controls include the inherited controls surrounding the data centers housing the servers and supporting hardware.

Identify the publicly-available URL:

https://gudid.fda.gov/gudid/

Note: web address is a hyperlink.

Does the website have a posted privacy notice?

Yes

Is the privacy policy available in a machine-readable format?

Yes

Does the website use web measurement and customization technology?

Yes

Select the type of website measurement and customization technologies is in use and if it is used to collect PII.

Session Cookies that do not collect PII.

Does the website have any information or pages directed at children under the age of thirteen?

No

Does the website contain links to non- federal government websites external to HHS?

No

Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?

N/A