US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

10/21/2016

OPDIV:

FDA

Name:

FDA CDER Sentinel

PIA Unique Identifier:

P-7320653-591636

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.

Contractor

Is this a new or existing system?

New

Does the system have Security Authorization (SA)?

Yes

Describe the purpose of the system.

Sentinel is a project sponsored by the FDA as part of an initiative to create an active safety surveillance system called the Sentinel System to monitor the safety of FDA-approved medical products. To accomplish this purpose, Sentinel uses pre-existing electronic healthcare data provided by multiple sources.

The overarching Sentinel Initiative is the FDA's response to the Food and Drug Administration Amendments Act of 2007 (FDAAA) requirement that the FDA work with public, academia, and private entities to develop a system to obtain relevant information from existing electronic health care data in order to assess the safety of approved medical products.

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

Sentinel uses pre-existing, de-identified electronic healthcare data from the various Sentinel Data Partners. Data Partners include participating health insurers, care providers and academic institutions. Initial data queries developed by FDA analysts are provided to the Data Partners and they provide responses in de-identified, summary format to an Operations Center which aggregates the data and provides it to the FDA.

A contractor, Harvard Pilgrim operates Sentinel and specifically, the Operations Center. Harvard Pilgrim contractors are not direct contractors and do not have FDA credentials. Participating Data Partners are sub-contractors with Harvard Pilgrim.

Most Sentinel activities focus on safety assessments, evaluation methods, or data. The fact that FDA requests and receives data on a particular product through Sentinel does not necessarily mean there is a safety issue with the product.

By design, all data providers must de-identify any data (remove direct patient/person identifiers) before providing it to the Operations Center. The Operations Center subsequently transmits de-identified information to FDA in response to queries submitted by FDA. In the event that person-level information (as opposed to more typical aggregated or cumulative data) is required for FDA analyses, Data Partners remove direct patient/person identifiers from the information conveyed to the Operations Center. If the Operations Center inadvertently receives direct patient identifiers, it will return or destroy the data immediately. All data that FDA receives is intended to be thoroughly de-identified before it reaches FDA.

When submitting data requests (aka queries), FDA users access Sentinel using a system-specific username and password. In order to register for an account, users must provide their first name, last name and e-mail address for creating an account to access the Sentinel portal. Administrators are responsible for creating Sentinel user accounts for FDA employees and direct contractors.

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

The Sentinel project provides FDA the ability to (1) work through the “nuts and bolts” of designing safety assessments using multiple existing electronic healthcare data systems; (2) develop and evaluate scientific methods to increase the precision of active health and safety surveillance efforts; and (3) identify and address barriers and challenges to building a practical, accurate, and timely system for active safety surveillance.

Sentinel uses de-identified pre-existing electronic healthcare data from multiple sources (the Data Partners). FDA may access the data available through Sentinel for a variety of reasons beyond assessing potential safety risks for a specific product. Some examples include determining a rate or count of an identified health outcome of interest, examining medical product use, or seeking to better understand the capabilities of the Sentinel project.

Sentinel employs a distributed data approach in which the individual Data Partner entities maintain physical and operational control over electronic data in their existing environments. This approach minimizes the need to share identifiable patient information. Additionally, each health care data system has unique characteristics, and use of a distributed system enables the Data Partners to perform analyses in their environment. By virtue of this process, unique system characteristics do not present a technical roadblock or require system redesign. The distributed data model thereby ensures an informed approach to interpreting queries and analytical results across multiple Data Partners.

The Operations Center coordinates all activities and queries with the Data Partners. FDA submits queries to the Operations Center which prepares and sends the appropriate analytical program that each Data Partner will run behind its own firewall. Each Data Partner will then submit de-identified aggregated results to the Operations Center. The Operations Center aggregates the data from each of the Data Partners and sends a final aggregated data report to the FDA. After the report has been finalized, it is posted on sentinelsystem.org. Data transfer between Data Partners and the Operations Center, and, between the Operations Center and the FDA is done by means of a secure web-based file sharing system.

When submitting data requests, FDA users access Sentinel using system-specific usernames and passwords. Users must provide a first name, last name and e-mail address in the processes of creating an account to the Sentinel portal. Users create their own passwords that must meet complexity standards. Administrators are responsible for creating Sentinel user accounts for FDA employees and direct contractors.

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

Usernames and Passwords

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

Employees

Vendor/Suppliers/Contractors

FDA users may include permanent and direct contractor employees. As a result of the data de-identification, no patient identifiers/PII is maintained within Sentinel.

How many individuals' PII is in the system?

500-4,999

For what primary purpose is the PII used?

The PII consists of usernames and passwords of system users which FDA uses to control system, access, use and security.

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 Food and Drug Administration Amendments Act of 2007 (FDAAA) amended the Federal Food, Drugs and Cosmetics Act to require the FDA to "establish collaborations with public, academic, and private entities ... to provide for advanced analysis of drug safety data ... and other information that is publicly available or is provided by" HHS and partners to its initiatives. Further, the FDAAA specifies that "[s]uch analysis shall not disclose individually identifiable health information when presenting such drug safety signals and trends or when responding to inquiries regarding such drug safety signals and trends." (See 21 U.S.C. 505(k)(4)(A) and (B).)

The security and privacy measures of the system including the use of usernames and passwords are required by the Federal Information Security Management Act (FISMA) and the statutes underlying OMB Circular A-130 for the secure and efficient use of government systems and resources.

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

No

Identify the sources of PII in the system.

Email

Government Sources

Within OpDiv

Identify the OMB information collection approval number and expiration date

Not applicable.

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.

No prior notice is required to receive de-identified data for research purposes. FDA and direct contractor and non-direct contractor employees are aware their username and password information will be collected in order for them to be given access to FDA information systems.

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.

Submission of PII is voluntary as that term is used by the Privacy Act. However, the submission of PII is necessary in order for users to access and use the system.

There is no method to opt not to submit PII. Permanent, direct contract and non-direct contract employees must provide their PII in order for the processing of administrative materials and to securely administer access to agency information and property such as the Sentinel system.

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

No such changes are anticipated. If the agency changes the collection, use, or sharing of PII data in this system, the affected individuals will be notified by the most efficient and effective means available and appropriate to the specific change(s). This may include a notice on the web site, or e-mail notice to the individuals. Because the health data in this system is thoroughly de-identified, notification would not be possible.

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.

Individuals who suspect their PII has been inappropriately obtained, used or disclosed in any FDA system have a number of avenues available to request to rectify the situation. Often, these individuals contact the office or division where they have determined that their information is held. Individuals may then make further requests for their information to be corrected or amended. FDA considers these requests and, if appropriate, makes the requested changes.

Employees with such concerns can additionally work with their supervisors, a 24-hour technical assistance line, FDA's Computer Security Incident Response Team, and other channels.

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

Because data providers de-identify the information before providing it the Operations Center and FDA, no reference model is available to FDA to facilitate re-assessing data integrity. Potential data integrity issues would be addressed by the source, i.e., the data providers.

FDA personnel are responsible for providing accurate information and may independently update and correct their information (username and password) at any time.

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

Users:

Users have access to their own system login credentials (username and password). Users will not have access to others' login credentials.

Administrators:

Administrators may be application administrators who require access to create and manage user accounts, but will not have access to users' self-created passwords.

Developers:

Developers may have limited access to usernames in the course of maintaining the systems or providing technical assistance.

Contractors:

Some developers may be direct contractors and will have access under the same circumstances as developers. Harvard Pilgrim contractors (not direct contractors) will have access to user PII other than passwords.

Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.

All access to Sentinel for users, administrators, developers and contractors require supervisor approval prior to the user gaining access. System access is reviewed on a quarterly basis to identify and remove unnecessary accounts.

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.

Management establishes roles for individual personnel, with role-based restrictions permitting access only to information that is required for each individual to perform his/her job.

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.

The FDA requires all agency personnel and direct contractors to complete FDA's IT Security and Privacy Awareness training at least once every 12 months. A portion of this training is dedicated to guidance on recognizing and safeguarding PII.

Describe training system users receive (above and beyond general security and privacy awareness training).

Additional on-the-job or informal training may be received.

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.

General Records Schedule (GRS) 3.2. Item 030, Disposition Authority: DAA-GRS-2013-0006-0003. Destroy when business use ceases.

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

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. Physical controls include that all system servers are located at FDA 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.

Identify the publicly-available URL:

https://www.sentinelsystem.org/

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 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?

No