US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

10/07/2016

OPDIV:

FDA

Name:

Mammography Program Reporting Information System

PIA Unique Identifier:
P-7220509-332067

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?
No

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

Other...

Describe in further detail any changes to the system that have occurred since the last PIA.
Routine updates and maintenance have occurred since the last PIA for this system.

Describe the purpose of the system.
Under the Mammography Quality Standards Act (MQSA), all mammography facilities must be accredited by an approved accreditation body, certified by the FDA, and inspected annually in order to legally provide mammography services in the United States. Mammography facility medical personnel must also meet qualification standards. The Mammography Program Reporting and Information System (MPRIS) is an automated system that FDA's Division of Mammography Quality Standards (DMQS) designed and developed to support implementation of the MQSA requirements. MPRIS stores information about inspections and accreditations for mammography facilities and is used to produce reports.

MPRIS provides a centralized repository of information that: (1) helps to ensure the quality, reliability, integrity, and accessibility of facility certification, inspection, and compliance data; (2) permits accurate tracking and monitoring of a facility's accreditation, certification, inspection, and compliance history; and (3) provides a flexible and secure system capable of supporting future changes in data requirements, and the expansion in data communications.

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

The information collected in the Mammography Program Reporting and Information System (MPRIS) includes the name and physical location of each mammography facility, along with the facility mailing address, telephone and facsimile numbers, the types and number of mammography equipment in use, and PII consisting of the names of facility personnel, including official contacts for accreditation, billing, and compliance matters.

The facility information is collected by FDA inspectors, FDA-approved accreditation bodies, and by State inspectors working under contract to FDA, in the course of mandatory annual facility inspections. This information is required by, and used in keeping with, the provisions of the MQSA and related FDA regulations (21 CFR Part 900) to contact the regulated facility regarding FDA matters, to determine their certification status, to schedule inspections, and to determine the compliance of the facility and facility personnel with the MQSA and related regulations.

The Center for Devices and Radiological Health (CDRH) Division of Mammography Quality Standards (DMQS) also collects information in MPRIS regarding the State inspectors working under contract with FDA. This data is obtained from State authorities at the time of contract signing, and it is limited to publicly-available information, including PII consisting of inspector name, office address, and office telephone and facsimile number. Submission of this information (PII) is not required by statute but is necessary in order for FDA to contact inspectors and provide technical support, equipment, and policy guidance when necessary.

Users are all FDA employees, and access the system using usernames and passwords.

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

CDRH employs the MPRIS to maintain inspection data and facility information, and, manage the inspection and reporting process. Information in MPRIS is shared with authorized FDA employees and contractors, and with the Centers for Medicare and Medicaid Services (CMS). No personal information is shared with CMS. CMS receives listings of facilities for reimbursement.

As described within this assessment, MPRIS is a centralized repository of information that: (1) helps to ensure the overall quality, reliability, integrity, and accessibility of facility certification, inspection, and compliance data by providing data edits, validation, and the security of a single integrated database; (2) permits accurate tracking and monitoring of a facility's accreditation, certification, inspection, and compliance history; and (3) provides a flexible and secure system that can expand to address future data submission and communications requirements. The PII collected is required and used for contact and inspection management purposes.

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

Mailing Address

Phone Numbers

Inspector ID number; work phone number, email and mailing address for points of contact as submitted by each individual.
FDA employee user credential (username and password)

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

Employees

Public Citizens

Business Partner/Contacts (Federal/state/local agencies)

"Employees" refers to FDA personnel including contract employees; "Public Citizens" refers to points of contact at mammography facilities; "Business Partners" includes state/local agency contacts.

How many individuals' PII is in the system?

100-499

For what primary purpose is the PII used?

The limited PII collected is required and used for contact and inspection management purposes. PII is shared only with authorized FDA employees and contractors; it is not disclosed outside FDA. PII in MPRIS is not matched against PII in other systems, and no other organization or systems are dependent on the PII in MPRIS. Individuals who have questions or complaints, or wish to correct their PII (contact information, ID number) may contact system or program management.

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.

42 U.S.C. 263b

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

No

N/A

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Email

Online

Government Sources

Within OpDiv

State/Local/Tribal

Identify the OMB information collection approval number and expiration date

0910-0309, August 31, 2016. Renewal package under review by OMB as of August 22, 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.

FDA employees are notified and consent to the agency's use of their information at the time of hire (HHS/FDA orientation and processing). External submitters of PII knowingly submit their information directly to FDA and are notified via the statutory requirements of the MQSA, form guidance and through FDA's privacy policies as permanently posted on FDA.gov.

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 PII in this system is submitted on a "voluntary" basis as that term is used by the Privacy Act. There is no opt-out process incorporated in this system regarding the administrative/contact PII submitted by individuals. The limited PII collected is required and used for contact and inspection management purposes. System users are advised at log in to the system that it is for use by authorized personnel only, that system use may be monitored and that by using MPRIS they consent to monitoring. Users are assigned a username and temporary password at the time accounts are created, and change the password before first using the system.

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

If FDA implements a major change to its use of MPRIS, the affected individuals will be notified electronically by e-mail directly to the individuals, to the facility, and/or to the State office(s) through which FDA contracts with the State inspectors.

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.

State inspectors and facility contacts may correct their PII data (name and work contact information) and submit any data use or sharing concerns by contacting the appropriate FDA/MPRIS office. Individuals who have questions or complaints, or wish to correct their PII, may contact system or program management. FDA personnel may raise concerns or correct information through FDA's Employee Resource Information Center or by contacting MPRIS management.

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

Accuracy is protected by providing an opportunity for user input. When an account is established, mailing, e-mail and phone number information can be updated by the user. There is no formal process for periodically reviewing this data. Integrity and availability are protected by security controls selected based on the sensitivity of the information in the system and appropriate guidance from the National Institute of Standards and Technology. Relevancy is ensured by not permitting the use of unused accounts. If an account is not accessed within 60 days, the password expires and liaisons are contacted to check the status of the user. Accounts no longer needed are inactivated.

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

Users:

Data submission and review; manage and track assignments

Administrators:

Monitor the system and manage access

Developers:

As necessary to alter, enhance the system

Contractors:

Submit inspection data (state inspectors are FDA contract employees)

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

Users who require access to the information system can only do so after obtaining supervisor approval.

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.

Supervisor will use the account creation form to limit access to the minimum necessary in order for the user to complete his/her job. The access list for the information system is also reviewed on a quarterly basis during which time users' access permissions are reviewed/adjusted, and unneeded accounts are purged from the system.

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 FDA personnel must complete annual Security and Privacy Awareness training.

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

Users receive system-specific training, are provided the HHS Rules of Behavior and may obtain additional privacy guidance from FDA's privacy office.

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.

CDRH maintains MPRIS records in accordance with FDA Records Control Schedule series 5200 and approved NARA citations N1-088-06-1, items 1.2.1, 1.2.2, 1.2.4-.6 and General Records Schedule 24, items 6a and 11a. These schedules specify different retention/deletion periods based on the type of record, e.g., 10 years after the relevant establishment goes out of business or product is withdrawn.

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

The information in MPRIS is protected by requiring users to receive training and agree to a set of Rules of Behavior, user identification, passwords, firewalls, virtual private network (VPN), encryption, intrusion detection system (IDS), guards, identification badges, key cards, cipher locks, closed circuit television. Other controls are also implemented as appropriate, in accordance with relevant guidance from the National Institute of Standards and Technology (NIST).