Privacy Impact Assessment (PIA): FDA - eNSpect - QTR1 - 2023 - FDA2078088

Date Signed: 2/6/2023

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

Status:	Approved	**PIA ID:**	1607484
PIA Name:	FDA - eNSpect - QTR1 - 2023 - FDA2078088	**Title:**	ORA Systems for Inspections, Recall, Compliance and Enforcement
OpDiv:	FDA		

PTA

PTA - 2:	Indicate the following reason(s) for this PTA. Choose from the following options.	New
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.	In support of FDA Office of Regulatory Affairs (ORA) inspection activities, the Electronic

		Inspection system (eNSpect) allows FDA Consumer Safety Officers (CSO) and FDA Consumer Safety Investigators (CSI) to work completely offline (no connection with the FDA network) on their mobile device (laptop and tablets) while they are performing their inspections at establishments regulated by the FDA. This is not a mobile device application, but a locally installed application on Windows laptops. eNSpect is one component of the overall ORA Systems for Inspections, Recall, Compliance and Enforcement (SIRCE). FDA has assessed the other SIRCE components in separate PIAs. The purpose of eNSpect is to support FDA investigators in performing inspections onsite at the physical locations of FDA-regulated establishments (firms) and provide records used by FDA employees in investigations of possible violation of laws enforced by the agency. The eNSpect system is comprised of both an online and an offline application for the FDA investigators to use in documenting their inspections including the generation of the FDA Establishment Inspection Report (EIR), documented in FDA Form 482 (Notice of Inspection) and FDA Form 483.
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.	eNSpect is used by FDA investigators during an inspection to collect data about the FDA-regulated establishment they are inspecting

		as well as the FDA investigator's observations and findings during the inspection. The observations and findings information is presented in a narrative included in legal documents developed by the FDA investigator. Observations and findings may include any type of information entered by the investigator to support and describe their inspection, observations and findings at the firm. Information collected by the FDA investigators as part of the inspection of FDA-regulated establishment includes: observations and findings, establishment (firm) name, firm address, firm type, FDA Establishment Identifier (FEI) number and inspection date as well as personally identifiable information (PII) about the Firm's point-of-contact (POC) including name(s) and the POC's title, phone number, email address and fax number. PII about Firm POCs is provided by the individual POC or by their employing firm and consist of work-related details only. This PII is provided in person at the time of inspection, or during initial and\or follow up contact with the firm. Additionally, eNSpect contains PII about FDA investigators as part of the inspection records and documentation (legal documentation): first name, last name, work phone number, work email address and work fax number. This PII about FDA personnel is obtained from other internal FDA systems such as the FDA's Active Directory, Enterprise Administrative Support Environment (EASE), and the ORA Operations Database. Investigators access the system via a single-sign-on (SSO) process using multi-factor authentication. eNSpect does not require, use, collect or maintain system-specific logon credentials (e.g., username and password).
PTA - 5A:	Are user credentials used to access the system?	No

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 eNSpect system enables the investigator or team of investigators to electronically coordinate

and share their work amongst themselves. This includes the recording, producing, labeling and organizing of all Establishment Inspection Report (EIR) documentation, evidence and exhibits resulting from the inspection including the FDA Form 483 Inspectional Observations (findings and citations) for the inspected establishment. The FDA Form 483 is issued to firms at the conclusion of an inspection in cases when an investigator has observed conditions that in their judgement may constitute violations of the Federal Food, Drug and Cosmetic Act and related Acts.

The types of inspections conducted include domestic and foreign inspections in support of compliance, consumer complaints, recalls and product safety surveillance. Establishments (Firms) include any and all Firms regulated by the FDA including Firms responsible for the manufacturing and processing of foods, feeds, drugs, medical devices and in-vitro diagnostic devices.

In using eNSpect, FDA inspection team members (investigators and their supervisors) may assign one or more team members to an eNSpect inspection assignment by selecting from a pop-up list of values. The list of values (FDA investigator names) is generated by an internal query within the eNSpect system. Additionally, an FDA supervisor can enter an investigator's name into the eNSpect operation inbox user interface to further filter the view of inspection assignment records in the inbox.

Additionally, eNSpect includes a team inspections feature that allows for more than one investigator to share and contribute their work during the inspection thereby eliminating team bottlenecks and otherwise necessary work to consolidate inputs from multiple investigators. Furthermore, eNSpect utilizes digital signatures (via the investigator's FDA Personal Identity Verification (PIV) card) as required on the FDA Form 483 and EIR documentation to streamline the signature gathering process between the FDA and inspected establishment.

After the FDA Consumer Safety Officer (CSO) and Consume Safety Inspector (CSI) return from their inspection, they are able to connect to the eNSpect online application through the FDA network via FDA's Single Sign On (SSO) authentication process to manage reports.

eNSpect inspections include information entered by the FDA investigators into free text fields supporting 483 citation observations, summary of inspection findings and inspection endorsement, as well as the EIR narrative report.

eNSpect is used to collect and maintain FDA-regulated establishment information and information about their main POC. The information includes Firm name, Firm address, Firm type, FDA Establishment Identifier (FEI) number and inspection date as well as the name(s) of the Firm's POC and the POC's Firm title, Firm phone number, Firm email address and Firm fax number. eNSpect also maintains the first and last name and work contact information of FDA investigators.

The information FDA maintains in eNSpect is shared internally within FDA for inspections, product recalls, compliance and enforcement purposes. No PII in the system is shared out of the system with any individuals or entities outside HHS.

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?	No
PTA - 14:	Does the system have a mobile application?	No
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 - 1:	Indicate the type(s) of personally identifiable information (PII) that the system will collect, maintain, or share.	Email Address Mailing Address Name Phone numbers Other - Free text Field - FDA Establishment Identifier (FEI) number and inspection date (potential PII), job title (within Firm) and work fax number are also forms of PII/potential PII that are collected.
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?	FDA/ORA uses the PII to manage inspection actions, accurately document an inspection for compliance, for business contact purposes, and in support of enforcement and analysis activities where inspection data is relevant.
PIA - 7:	Identify legal authorities governing information use and disclosure specific to the system and program.	Federal Food, Drug, and Cosmetic Act, 21 U.S.C. 374; Public Health Service Act, 42 U.S.C. 262-264.
PIA - 8:	Are records in the system retrieved by one or more PII data elements?	Yes
PIA - 8A:	Please specify which PII data elements are used to retrieve records.	All of the PII elements in the system that are associated with firm POCs are used to retrieve records; these retrievals are rare and are for the purpose of efficient communication (e.g., Firm POC contacts inspector for follow up directly).
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.	SORN 1: 09-10-0002, Regulated Industry Employee Enforcement Records
PIA - 9:	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains In-person Government Sources

		Within the OPDIV Non-Government Sources Private Sector Other
PIA - 10:	Is there an Office of Management and Budget (OMB) information collection approval number?	No
PIA - 11:	Is the PII shared with other organizations outside the system's Operating Division?	No
PIA - 12:	Is the submission of PII by individuals voluntary or mandatory?	Voluntary
PIA - 13:	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	Establishment personnel provide PII voluntarily or their employing firm provides it. They may work with their employer if they do not wish to have their PII submitted. They may also object or discuss inspection observations with the FDA representative during the inspection or by contacting the FDA after the inspection. FDA personnel are required to provide their name and work contact information in order to get authorization to access the system.
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 practices change with regard to the collection or use of PII in eNSpect, the agency will provide any required notice and obtain consent from individuals. Notice procedures may include Federal Register notices, hard copy mail to individuals, adding or updating online notices and disclaimers, or using other available technological means for notification and consent.
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.	Personnel may raise concerns and/or submit data corrections through supervisory channels and FDA's Employee Resource and Information

		Center (ERIC). Individuals who are members of the inspected establishment (Firm) may contact FDA through numerous paths such as email, phone and standard mail avenues (all listed on fda.gov). Additionally, there is a review process during the inspection that allows for a firm point of contact to review the final inspection reports and identify anything that they feel is inaccurate. All FDA personnel are required to rapidly report the potential or suspected unauthorized access or use of PII to the Cybersecurity and Infrastructure Operations Coordination Center (CIOCC). Any individual with a concern about their PII may contact the FDA Privacy program using information provided on FDA.gov.
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.	All PII is relevant. Forms and processes are designed to collect only PII that is necessary for the relevant agency activity. PII about a point of

		contact is necessary to communicate with regulated establishments. PII (name and work contact data) is provided by the establishment or the individual establishment employee, and the individual and/or establishment is responsible for providing accurate information. Accuracy is ensured by individual review of inspection reports and correcting data in the course of ORA's use of the system/information, e.g., updating name and phone number for entity point of contact. Firms/individuals may amend their submitted contact information by contacting FDA. FDA personnel may correct/update their information themselves. Integrity and availability are protected by security controls selected and implemented in the course of providing the system with an authority to operate (ATO). Controls are selected based on NIST guidance concerning the ATO process, appropriate to the system's level of risk as determined using the National Institute of Standards and Technology (NIST's) Federal Information Processing Standards (FIPS) 199.
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: Performing and documenting FDA Inspections. Administrators: Administrators have access to PII in the course of performing analysis of historical activities and to review work in process. Developers: Developers have access to PII to perform level 3 Helpdesk support Contractors: Helpdesk Direct Contractors have access to PII to perform level 1 and 2 Helpdesk support activities.

PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	System access requests are reviewed and approved by the system/business owner along with the eNSpect management team. System accounts are reviewed on a regular basis to determine if access is still required for each user. Access is granted and restricted at the individual level as appropriate to the individual's duties (role-based 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.	When system accounts are created for personnel, supervisors determine the scope of required access and apply the minimum information system access that is required for the user to complete his/her job. The access list for the information system is reviewed on a quarterly basis and users' access permissions are reviewed/adjusted, and unneeded accounts are purged from the system.
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 personnel complete mandatory security and privacy awareness training at a minimum of once a year. Completion is tracked by the Office of Digital Transformation (ODT).
PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	Users receive system-specific training, review and adhere to the Rules of Behavior, and may obtain additional privacy guidance from the agency's privacy officials.
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).	eNSpect records are maintained under the National Archives and Records Administration (NARA) Citation N1-088-09-1, FDA file code 7300 series, for Establishment Inspections and Compliance Action Files. Records are destroyed 10 years after classification of an inspection as "no action" or "voluntary action" indicated, and 30 years after close of a case where official action was indicated
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 uses of firewalls; access controls such as usernames and passwords; and regular testing of information technology systems.

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 NIST's Special Publication 800-53, as determined using Federal Information Processing Standard (FIPS) 199.