PI Dashboard

1. OPDIV	National Institutes of Health
2. PIA Unique Identifier	P-5860043-506903
2a. Name	OD ORS PI Dashboard/ HealthRx Nexus
3. The subject of this PIA is which of the following?	Minor Application (child)
3a. Identify the Enterprise Performance Lifecycle Phase of the system.	Operational
3b. Is this a FISMA-Reportable system?	No
4. Does the system include a Website or online application available to and for the use of the general public?	No
Accept / Reject Status	Accept
Question 4 Comment	
5. Identify the operator.	Contractor
6. Point of Contact (POC)	
POC Title	Chief, Biorisk Management Branch, DOHS, ORS
POC Name	Jeffrey Potts
POC Organization	Division of Occupational Health and Safety
POC Email	pottsj@mail.nih.gov
POC Phone	301-402-7460
Accept / Reject Status	Accept
Question 6 Comment	

7. Is this a new or existing system?	Existing
8. Does the system have Security Authorization (SA)?	Yes
Accept / Reject Status	Accept
Question 8 Comment	
8a. Date of Security Authorization	03/31/2018
9. Indicate the following reason(s) for updating this PIA. Choose from the following options.	Annual review
Other	
Accept / Reject Status	Undefined
Question 9 Comment	
10. Describe in further detail any changes to the system that have occurred since the last PIA.	The System has undergone moderate changes to enhance functionality and increase business functions. For example, to meet changes necessary for the mass flu vaccine clinic (Foil the Flu) boarding pass, self-scheduling, and text notification functions were added. Other minor changes included moving or eliminating radio buttons or rephrasing questions in a safety survey. New modules were added in the system which will expedite access approvals to certain components as well as enhanced capabilities for reporting metrics from the system.
Accept / Reject Status	Accept
Question 10 Comment	
11. Describe the purpose of the system.	HealthRx Nexus collects, stores and manages occupational safety and health data to assist with ensuring regulatory compliance and auditing purposes.

	Research and regulatory data supporting the National Institutes of Health (NIH) Intramural Research Programs for all 27 Institutes and Centers (ICs) is managed in HealthRx Nexus. HealthRx Nexus connects research stakeholders by increasing safety and efficiency, streamlining submission and approval, and enhancing customer service for researchers. Its paperless registration management is both secure and accessible, which saves time, money, and space - and gets research online faster. PI-Dashboard empowers Principle Investigators (PI)s to track and manage bio-safety related activity more effectively so they can focus on research.
Accept / Reject Status	Accept
Question 11 Comment	
12. Describe the type of information the system will collect, maintain (store), or share. (Subsequent questions will identify if this information is PII and ask about the specific data elements.)	HealthRx Nexus is a database and workflow system supporting the NIH Division of Occupational Health and Safety which contains research and regulatory data and workflow modules (human pathogens, recombinant nucleic acids, dual use review, asbestos, respiratory protection laboratory audit, etc.). Data is entered via a government website interface utilizing NIH dual authentication. HealthRx Nexus stores limited Personally Identifiable Information (PII) of employees and direct contractors. This PII is imported from the National Institutes of Health Enterprise Directory (NED) and includes name, email address, phone number, and mailing address. The PII is only used to manage workflows, grant access, and to provide stakeholders with a channel of communication. NED has its own approved PIA on record, including all legal authorities documented. HealthRx Nexus uses specific login information to assign permissions/user roles which is considered Personally Identifiable Information (PII). However, this is done by using the NIH Identity, Credential, and Access Management Services: Identity Management Services (IMS), formally known as the Active Directory (AD), which combines the identity and authentication tools and capabilities used throughout the NIH

	enterprise. The IMS has its own approved PIA on record, including all legal authorities documented.
Accept / Reject Status	Accept
Question 12 Comment	
13. Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.	The system manages occupational safety and health data for regulatory compliance and auditing purposes. Research and regulatory data supporting the National Institutes of Health (NIH) Intramural Research Programs for all 27 Institutes and Centers (ICs). The system connects research stakeholders by increasing safety and efficiency, streamlining submission and approval, and enhancing customer service for researchers. Its paperless registration management is both secure and accessible, which saves time, money, and space - and gets research online faster. PI-Dashboard empowers Principle Investigators (PI)s to track and manage bio-safety related activity more effectively so they can focus on research. HealthRx Nexus is a database and workflow system supporting the NIH Division of Occupational Health and Safety which contains research and regulatory data and workflow modules (human pathogens, recombinant nucleic acids, dual use review, asbestos, respiratory protection, laboratory audit, etc.). Data are entered via a government website interface utilizing NIH dual authentication. The system holds limited Personally Identifiable Information (PII) of employees and direct contractors. This PII is imported from the National Institutes of Health Enterprise Directory (NED) and includes name, email address, phone number, and mailing address. The PII is only used to manage workflows, grant access, and to provide stakeholders with a channel of communication. NED has its own approved PIA on record, including all legal authorities documented. The system uses specific login information to assign permissions/user roles which is considered Personally Identifiable Information (PII). However, this is done by using the NIH Identity, Credential, and Access

	Management Services: Identity Management Services (IMS), formally known as the Active Directory (AD), which combines the identity and authentication tools and capabilities used throughout the NIH enterprise. The IMS has its own approved PIA on record, including all legal authorities documented.
Accept / Reject Status	Accept
Question 13 Comment	
14. Does the system collect, maintain, use or share PII?	Yes
Accept / Reject Status	Accept
Question 14 Comment	
15. Indicate the type of PII that the system will collect or maintain.	Name, E-Mail Address, Phone Numbers, Mailing Address, Employment Status, medical notes, DOB
Accept / Reject Status	Accept
Question 15 Comment	
16. Indicate the categories of individuals about whom PII is collected, maintained or shared.	Employees, Contractors
Accept / Reject Status	Accept
Question 16 Comment	

17. How many individuals' PII is in the system?	5,000-9,999
Accept / Reject Status	Accept
Question 17 Comment	
18. For what primary purpose is the PII used?	Employee contact and tracking for regulatory compliance and risk management. Certain information is utilized to ensure appropriate medical services and surveillance programs are offered to federal staff.
Accept / Reject Status	Accept
Question 18 Comment	
19. Describe the secondary uses for which the PII will be used (e.g. testing, training or research)	N/A
Accept / Reject Status	Accept
Question 19 Comment	
20. Describe the function of the SSN.	N/A
Accept / Reject Status	Accept
Question 20 Comment	
20a. Cite the legal authority to use the SSN.	N/A
21. Identify legal authorities governing information use and disclosure specific to the system and program.	42 U.S.C 241; 5 U.S.C. 7902; 42 U.S.C. 2201

22. Are records on the system retrieved by one or more PII data elements?	Yes
Accept / Reject Status	Accept
Question 22 Comment	
22a. Identify the number and title of the Privacy Act System of Records Notice (SORN) that is being used to cover the system or identify if a SORN is being developed.	
Published:	SORN: 09-25-0166 Administration: Radiation and Occupational Safety and Health Management Information Systems
Published:	
Published:	
In Progress	Undefined
23. Identify the sources of PII in the system.	In-Person, Hard Copy: Mail/Fax, Email, Online, Within the OPDIV, Other Federal Entities
Accept / Reject Status	Accept
Question 23 Comment	
23a. Identify the OMB information collection approval number and expiration date.	An OMB collection approval number is not needed as PI-Dashboard only uses the PII of federal employees for internal use only.
24. Is the PII shared with other organizations?	Yes
Accept / Reject Status	Accept
Question 24 Comment	

24a. Identify with whom the PII is shared or disclosed and for what purpose.	
Within HHS	Yes
	Centers for Disease Control and Prevention for regulatory compliance
Other Federal Agency/Agencies	Yes
	Occupational Health and Safety Administration for regulatory compliance
State or Local Agency/Agencies	No
Private Sector	No
24b. Describe any agreements in place that authorizes the information sharing or disclosure (e.g. Computer Matching Agreement, Memorandum of Understanding (MOU), or Information Sharing Agreement (ISA)).	No formal agreements exist but since the NIH is a regulated entity we must comply with federal regulations and provide information when necessary or as is described in the applicable Code of Federal Regulations (CFR).
24c. Describe the procedures for accounting for disclosures.	Written requests to the System Owner are reviewed to determine if a record exists. The requester must also verify his or her identity by providing either a notarization of the request or a written certification and understands that the knowing and willful request for acquisition of a record under false pretenses is a criminal offense. Information is sanitized and PII is either removed or redacted prior to disclosure unless required by regulation.
25. Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain	All persons who enter in business relationships with the National Institutes of Health are fully informed in writing prior to the beginning of the transaction that personally identifiable information (PII) is required in order to proceed. Information that is pulled from the NIH Enterprise

the reason.	Directory (NED) is voluntarily submitted and entered by an Administrative Officer or by the employee. NED has its own approved PIA on record, including all legal authorities documented.
Accept / Reject Status	Accept
Question 25 Comment	
26. Is the submission of PII by individuals voluntary or mandatory?	Voluntary
Accept / Reject Status	Accept
Question 26 Comment	
27. 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.	Information is required to meet regulatory requirements; respond to emergencies and risk reduction purposes. Information has to be collected in order to provide contact information for biological research being performed at NIH. If individuals do not want to give their information, they cannot participate in NIH research. For PII that is downloaded from the NIH Login and the NIH Identity, Credential, and Access Management Services: Identity Management Services (IMS), formally known as the Active Directory (AD); individuals are notified of the collection and use of the data as part of the hiring process. This is a requirement of potential job applicants seeking employment at NIH. Both Systems maintain their own PIAs and are responsible for providing methods for individuals to opt-out of the collection or use of their PII.
Accept / Reject Status	Accept
Question 27 Comment	
28. Describe the process to notify and obtain consent from	PII is downloaded in HealthRx Nexus from NED, NIH Login, and the NIH Identity, Credential, and Access Management Services: Identity Management Services

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.	(IMS), formally known as the Active Directory (AD). Individuals are notified of major changes that occur in the NED, NIH Login, and IMS through official notices sent out or an Administrative Officer updates or changes PII within the two systems. Project staff send all system users notices when major changes to the system occur. Supervisors are notified when changes in user profiles/accounts are requested. Notices are in the form of email.
Accept / Reject Status	Accept
Question 28 Comment	
29. 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.	Individuals have access to their information at all times; in some cases they may make changes to the data themselves. In other cases, they may make their request verbally or in writing to system administrators.
Accept / Reject Status	Accept
Question 29 Comment	
30. Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy. If no processes are in place, explain why not.	Data is used daily for business purposes; annual review of the data/information is required to be performed by the individuals whose PII is contained in the system.
Accept / Reject Status	Accept

Question 30 Comment	
31. Identify who will have access to the PII in the system and the reason why they require access.	
Users	Yes
	Update data
Administrators	Yes
	For management of occupational health and safety programs.
Developers	Yes
	For update of software and troubleshooting problems.
Contractors	Yes
	Direct Contractors for updating software and troubleshooting problems and for accident/injury trend analysis or other required analysis
Others	No
32. Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Access roles are granted by program managers only for information/data pertinent to the individuals need.
Accept / Reject Status	Accept
Question 32 Comment	
33. 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.	Data is stored in modules and separate data sets to which limited access is granted only for business necessity. Dual authentication through NIH Login is required. Following login, system user's privileges are verified through the use of the NIH Identity, Credential, and Access Management Services: Identity Management Services (IMS), formally known as the Active Directory (AD), and has its own approved PIA on record, including

	all legal authorities documented.
Accept / Reject Status	Accept
Question 33 Comment	
34. 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 NIH Security Awareness Training course is used to satisfy this requirement. According to NIH policy, all personnel who use NIH applications must attend security awareness training every year. There are four categories of mandatory IT training (Information Security, Counterintelligence, Privacy Awareness, and Records Management). Training is completed on the http://irtsectraining.nih.gov site using valid NIH credentials.
Accept / Reject Status	Accept
Question 34 Comment	
35. Describe training system users receive (above and beyond general security and privacy awareness training).	System tutorials are available for end users to review on their own time but are not required training.
Accept / Reject Status	Accept
Question 35 Comment	
36. Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?	Yes

Accept / Reject Status	Accept
Question 36 Comment	
37. Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific records retention schedules.	Records are maintained within HealthRx Nexus for a time of no less than 30 years after monitoring is conducted in accordance with NARA record retention schedule: 2.7.040, Workplace environmental monitoring and exposure records; DAA-GRS-2017-0010-0004 Records are maintained within HealthRx Nexus for a time of no less than six years after a password is altered or a user account is terminated in accordance with NARA record retention schedule: 3.2.031, System access records; Systems requiring special accountability for access; DAA-GRS-2013-0006-0004 Records are maintained within HealthRx Nexus for one year after the system is superseded by a new iteration or when no longer needed for agency/Information Technology (IT) administrative purposes to ensure a continuity of security controls throughout the life of the system in accordance with NARA record retention schedule: 3.2.010, Systems and data security records: DAA-GRS-2013-0006-0001
Accept / Reject Status	Accept
Question 37 Comment	
38. Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.	Administrative Controls: System users are approved by HealthRx Nexus management for access based on their technical or functional role within the system. Technical Controls: Access to the system is controlled by NIH log-in which authenticates the user prior to granting access. Access level and permissions are controlled by the system and based on user, role, and/or organizational unit. All servers have been configured to remove all unused applications and system files and all local account access except when necessary to manage the system and maintain

	integrity of data. Physical Controls: The servers reside in the Center for Information Technology (CIT) Computer Room where policies and procedures are in place to restrict access to the machines. This includes guards at the front door and entrance to the machine room.
Accept / Reject Status	Accept
Question 38 Comment	
39. Identify the publicly-available URL.	https://oms.ors.nih.gov
Accept / Reject Status	
Question 39 Comment	
40. Does the website have a posted privacy notice?	Yes. The login page contains a link to the NIH Privacy Policy
Accept / Reject Status	
Question 40 Comment	
40a. Is the privacy policy available in a machine-readable format?	Unknown
41. Does the website use web measurement and customization technology?	No
Accept / Reject Status	

Question 41 Comment	
41a. Select the type of website measurement and customization technologies is in use and if it is used to collect PII. (Select all that apply).	
Web Beacons	No
Collects PII?	No
Web Bugs	No
Collects PII?	No
Session Cookies	No
Collects PII?	No
Persistent Cookies	No
Collects PII?	No
Other ...	No
Collects PII?	No
42. Does the website have any information or pages directed at children under the age of thirteen?	No
Accept / Reject Status	
Question 42 Comment	
42a. 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?	No (N/A)
43. Does the website contain links to non-	No

federal government websites external to HHS?	
Accept / Reject Status	
Question 43 Comment	
43a. Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?	There are no links to external sites from the application.
REVIEWER QUESTIONS: The following section contains Reviewer Questions which are not to be filled out unless the user is an OPDIV Senior Officer for Privacy.	
1. Are the questions on the PIA answered correctly, accurately, and completely?	Undefined
Reviewer Notes	
Accept / Reject Status	Undefined
Question 1 Comment	
2. Does the PIA appropriately communicate the purpose of PII in the system and is the purpose justified by appropriate legal authorities?	Undefined
Reviewer Notes	
Accept / Reject Status	Undefined

Question 2 Comment	
3. Do system owners demonstrate appropriate understanding of the impact of the PII in the system and provide sufficient oversight to employees and contractors?	Undefined
Reviewer Notes	
Accept / Reject Status	Undefined
Question 3 Comment	
4. Does the PIA appropriately describe the PII quality and integrity of the data?	Undefined
Reviewer Notes	
Accept / Reject Status	Undefined
Question 4 Comment	
5. Is this a candidate for PII minimization?	Undefined
Reviewer Notes	
Accept / Reject Status	Undefined
Question 5 Comment	
6. Does the PIA accurately identify data retention procedures and records retention schedules?	Undefined

Reviewer Notes	
Accept / Reject Status	Undefined
Question 6 Comment	
7. Are the individuals whose PII is in the system provided appropriate participation?	Undefined
Reviewer Notes	
Accept / Reject Status	Undefined
Question 7 Comment	
8. Does the PIA raise any concerns about the security of the PII?	Undefined
Reviewer Notes	
Accept / Reject Status	Undefined
Accept / Reject Status	Undefined
Question 8 Comment	
9. Is applicability of the Privacy Act captured correctly and is a SORN published or does it need to be?	Undefined
Reviewer Notes	
Accept / Reject Status	Undefined
Accept / Reject Status	Undefined
Question 9 Comment	
10. Is the PII appropriately limited	Undefined

for use internally and with third parties?	
Reviewer Notes	
Accept / Reject Status	Undefined
Question 10 Comment	
11. Does the PIA demonstrate compliance with all Web privacy requirements?	Undefined
Reviewer Notes	
Accept / Reject Status	Undefined
Question 11 Comment	
12. Were any changes made to the system because of the completion of this PIA?	Undefined
Reviewer Notes	
Accept / Reject Status	Undefined
Question 12 Comment	
General Comments	This component is under the Security and Emergency Response (SER) General Support System, whose Universal Unique Identifier (UUID) is: 16DD51AF-CC36-4BA9-A67D-C787BBB1100F.
Status and Approvals	
IC Status	IC Approved
OSOP Status	HHS Approved
OPDIV Senior Official for Privacy Signature	
HHS Senior Agency	

Official for Privacy	