Attachment 25 –
OCISO approval for the collection of PII

Save

Privacy Impact Assessment Form

v 1.47.4

Status Draft | Form Number F-25337 | Form Date 2/26/2019 8:46:16 AM

	Question	Answer
1	OPDIV:	CDC
2	PIA Unique Identifier:	P-6902544-932285
2a	Name:	Modernization Platform (MPN)
3	The subject of this PIA is which of the following?	○ General Support System (GSS) ◉ Major Application ○ Minor Application (stand-alone) ○ Minor Application (child) ○ Electronic Information Collection ○ Unknown
3a	Identify the Enterprise Performance Lifecycle Phase of the system.	Operations and Maintenance
3b	Is this a FISMA-Reportable system?	○ Yes ◉ No
4	Does the system include a Website or online application available to and for the use of the general public?	◉ Yes ○ No
5	Identify the operator.	◉ Agency ○ Contractor
6	Point of Contact (POC):	POC Title: Associate Director for IT POC Name: Mike Loudermilk POC Organization: CDC/NIOSH/OD POC Email: MLoudermilk@cdc.gov POC Phone: 404.498.1988
7	Is this a new or existing system?	◉ New ○ Existing
8	Does the system have Security Authorization (SA)?	○ Yes ◉ No
8b	Planned Date of Security Authorization	August 9, 2019 ☐ Not Applicable

Save

11	Describe the purpose of the system.	Modernization Platform (MPN) is a strategic effort to align existing National Institute for Occupational Safety and Health
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.)	MPN will maintain information such as social security numbers (SSN), names, email, address, phone, medical notes, certificates, date of birth (DOB), photographic identifiers,
13	Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.	The MPN helps to store and share information amongst the NIOSH divisions which are located in various states. The information collected is accessed by authorized NIOSH
14	Does the system collect, maintain, use or share PII?	(•) Yes ( ) No
15	Indicate the type of PII that the system will collect or maintain.	[X] Social Security Number [X] Date of Birth [X] Name [X] Photographic Identifiers [ ] Driver's License Number [X] Biometric Identifiers [ ] Mother's Maiden Name [ ] Vehicle Identifiers [X] E-Mail Address [X] Mailing Address [X] Phone Numbers [X] Medical Records Number [X] Medical Notes [ ] Financial Account Info [X] Certificates [ ] Legal Documents [ ] Education Records [ ] Device Identifiers [ ] Military Status [X] Employment Status [ ] Foreign Activities [ ] Passport Number [ ] Taxpayer ID Demographic info
16	Indicate the categories of individuals about whom PII is collected, maintained or shared.	[X] Employees [X] Public Citizens [X] Business Partners/Contacts (Federal, state, local agencies) [X] Vendors/Suppliers/Contractors [X] Patients Other: Publication Authors, Respirator Manufacturers seeking approval.
17	How many individuals' PII is in the system?	1,000,000 or more

Save

18	For what primary purpose is the PII used?	MPN collects external users' business contact information (email and phone number) for account set up and user support. MPN collects and maintains identifying information about the workers involved in the safety incident such as participants' names to ensure collected data is associated with the correct person. DOB is collected to understand any relationship between age and safety. Medical information (medical notes, medical records number, biometric identifiers) is collected to understand the safety and health risks of certain tasks and/or environments.	
19	Describe the secondary uses for which the PII will be used (e.g. testing, training or research)	Secondary uses for collecting PII include informing workers of study findings, analyzing data, administering surveys, contacting participants, verifying the miner's identity, to keep records of procedures performed within the system, and for user account setup and user support.	
20	Describe the function of the SSN.	MPN uses miner's SSN to search for data, verify identity, and group radiographs taken during a miner's lifetime. SSN is also used in determining whether a match is for a particular worker. The set of information which MPN and the data source have in common typically consists of SSN, name, date of birth, and gender. These fields are used to ascertain whether a linked record for a worker is a true match, a false match, or whether it remains unclear. Without the SSN, many of these determinations would be impossible.	
20a	Cite the **legal authority** to use the SSN.	Federal Mine Safety and Health Act, Sections 203 and Occupational Safety and Health Act, Section 20	
21	Identify **legal authorities** governing information use and disclosure specific to the system and program.	Occupational Safety and Health Act, Section 20, "Research and Related Activities" (29 U.S.C. 669); Federal Mine Safety and Health Act of l977, Sections 203, "Medical Examinations" and 50l, "Research" (30 U.S.C. 843, 95l); Public Health Service Act, Section 301, "Research and Investigation" (42 U.S.C. 241).	
22	Are records on the system retrieved by one or more PII data elements?	(●) Yes ( ) No	
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: 09-20-0149 | Morbidity Studies in Coal Mining, Metal and Non-metal Mining and General Industry. Published: Published: ☐ In Progress	

Save

23	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains ☒ In-Person ☒ Hard Copy: Mail/Fax ☒ Email ☒ Online ☐ Other Government Sources ☒ Within the OPDIV ☒ Other HHS OPDIV ☒ State/Local/Tribal ☐ Foreign ☒ Other Federal Entities ☐ Other Non-Government Sources ☒ Members of the Public ☐ Commercial Data Broker ☒ Public Media/Internet ☒ Private Sector ☐ Other
23a	Identify the OMB information collection approval number and expiration date.	OMB 0920-0953 Expires 08/31/2021 OMB 0920-0260, Expiration: 10/31/2020
24	Is the PII shared with other organizations?	◉ Yes ○ No

Save

24a	Identify with whom the PII is shared or disclosed and for what purpose.	☐ Within HHS ☒ Other Federal Agency/Agencies PII is provided to allow users to contact the publication author with questions/comments. The Mine Safety and Health Administration (MSHA) may be provided PII when needed, as NIOSH runs the Coal Workers' Health Surveillance Program (CWHSP) on their behalf. PII is provided to IRS for matching with their database in order to identify addresses for workers. PII is also provided to Department of Energy in order to obtain additional exposure data and study data. ☒ State or Local Agency/Agencies PII is provided to allow users to contact the publication author with questions/comments. PII is also provided to the State statistic offices and state cancer registries. ☒ Private Sector PII is provided to allow users to contact the publication author with questions/comments. Analysis files not containing direct identifiers may be shared with collaborators or researchers interested in replicating the study, either through a data use agreement or at a research data center. Lab testing with Clinical Laboratory Improvement Amendments (CLIA) certified lab

Save

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)).	Agreements are in place for data sharing as follows: 1) Data exchanged with National Death Index (NDI) is governed by the NDI process which includes an application process with protocol review of new studies. 2) Data exchanged with the Internal Revenue Service (IRS) is governed Under Title 26 – Internal Revenue Code 6103(m)(3), (https://www.irs.gov/irm/part11/irm_11-003-029) as amended (Appendix A) and Public Law 96-128, title V, Sec. 502, as amended, (http://thomas.loc.gov/cgi-bin/bdquery/z?d096:HR02282:@@@D&summ2=m&). NIOSH has been granted authority for this type of search and has been vetted by IRS to gain access and the use of their secure FTP site. 3) Data exchanged with Department of Energy (DOE) Inter-agency Agreement to collect study records from the various sites. 4) Data exchanged with state Vital Records departments are governed by an approval process with each state at the time requested. 5) Data exchanged with state cancer registries are governed by an approval process with each state at the time requested. 7) Study analysis files not containing direct identifiers are governed by Data Use Agreements or by restricted access through National Center for Health Statistics (NCHS's) Research Data Center.
24c	Describe the procedures for accounting for disclosures	Health Management Systems (HMS) Federal has established the International Organization for Standardization (ISO) 9001 procedures for accounting for disclosures under this system. This is maintained by the system owner. Within this disclosure ledger includes the date, the name (the address if known) of the entity of the receiving person or agency, a brief description of the information disclosed, and a brief purpose of the disclosure (or a copy of the disclosure request). This ledger is captured in a spreadsheet.
25	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 Miner Identification Form explains how the miner information will be kept private and requires them to sign granting NIOSH permission to collect and use the data when requesting a chest radiograph or pulmonary function test. When voluntarily signing up for an account, individuals provide business contact information. The website form describes the information collection and the use of PII. Users requesting access to the system for a specific role will be notified during the request either verbally or by email that their user Id will be stored. New employees are notified via email or verbally that their information will be stored.

Save

26	Is the submission of PII by individuals voluntary or mandatory?	(•) Voluntary ( ) Mandatory	
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.	Participation is voluntary and initiated by the users. Users opting to participate are required to provide business contact information as needed for account setup and user support. Once established, users can opt out by contacting eidtechinfo@cdc.gov and their account will be disabled.	
28	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.	Users are notified of system updates via the email address they provide. Major changes in the use of PII are not anticipated and have not occurred. No consent process has been developed.	
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.	If PII has been inappropriately obtained, used, or disclosed, or if the PII is inaccurate, an individual can contact the systems program manager at eidtechinfo@cdc.gov. Concerns about PII can be directed to NIOSH MPN administrators at nioshpia@cdc.gov. The administrators will direct the concern to the system security steward who will reach out to the individual and division management, NIOSH's Information System Security Officer, and CDC's Privacy Office for an appropriate resolution.	
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.	PII contained in the system is reviewed by MPN administrators weekly and any incorrect information is remedied. Additionally, users or authors may request their information be updated by sending an email to the system administrators. Integrity checks include: the data entry staff verify that PII matches the form when entering the data, entered data are compared to appropriate valid ranges of values, databases are designed to eliminate redundancies, and database constraints require values for critical fields and disallow invalid values. Workers' addresses are updated prior to notifications. Users may update their email address and phone number by sending updates to eidtechinfo@cdc.gov. Reviews are conducted by NIOSH's Project Manager.	
31	Identify who will have access to the PII in the system and the reason why they require access.	☒ Users	Program researchers will have access to their program's PII data in order to conduct analysis.
		☒ Administrators	For creating user accounts and communicating system status and providing user support.
		☐ Developers	
		☒ Contractors	Direct contractors serving as users administrators.
		☐ Others	

Save

32	Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	MPN utilizes Role Based Access Control (RBAC) that enforces the most restrictive permissions for authorized users based on their role. The Business Stewards determine which users can
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.	MPN personnel are identified at the project level by role, and only appropriate personnel with the requisite skills and knowledge are assigned to the project in the required role. System users and administrators are given access based on the principles of least privilege. Least Privilege model is applied, ensuring privilege levels no higher than necessary to accomplish required functions.
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.	All users complete Security and Privacy Awareness Training at least annually.
35	Describe training system users receive (above and beyond general security and privacy awareness training).	The Division of Field Studies and Engineering (DFSE) annually provides 308(d) training that includes Confidentiality as well as Privacy Act and security training. System administrators complete HHS Role Based Training at least annually. Freedom of Information (FOIA) and Privacy Act Training
36	Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?	(●) Yes ( ) No
37	Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific records retention schedules.	NIOSH handles and retains information system output and retention in accordance with the CDC Records Management Policy. CDC Records Control Schedule and other applicable record scheduling procedures prescribed by the General Records Schedule (GRS) and National Archives and Records Administration (NARA). System stewards consult with the CDC Records Manager to identify applicable records scheduling requirements and otherwise manage electronic records. Records Schedule 16, Item 14 Records Schedule N1-442-09-1, item 3 (4-57) Records Schedule is N1-442-09-1, item 2 Records Schedule N1-GRS-98-2 item 23 Records Schedule CDC N1-442-2009-01, item 3 and 4 Records Schedule N1-442-09-1 GRS 20.2D

Save

38	Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.	Administrative: only authorized employees can access using PIV card and system authentication. The business steward authorizes new users for the system. Data is secured by Active Directory and access is only granted to users authorized by the business steward. Data is stored on an encrypted database server. The servers and hard-copy records reside in secured facilities which require PIV card access. Comprehensive security plans are formalized through the Security Assessment and Authorization (SA&A) process to validate compliance with Federal Information Security Management Act (FISMA) requirements. Technical: both database layer and application layer access is controlled by PIV card (network user credentials) to prevent unauthorized access. PII is secured on the CDC network using network shares and Server databases that limit access to the appropriate staff. The network is protected with firewalls, and intrusion detection systems. All users complete Security and Privacy Awareness Training at least annually. Physical: Hosted and stored on the consolidated web server and database server which is located in a locked secure CDC facility, secured with guards, ID badges, key cards and closed circuit television (CCTV) with access only by authorized badged staff or escorted visitors.
39	Identify the publicly-available URL:	MPN is a platform framework that involves multiple URLs. https://wwwn.cdc.gov/HHERequest https://wwwn.cdc.gov/niosh-statedocs/Default.aspx https://www.cdc.gov/niosh/topics/NOMS/ https://wwwn.cdc.gov/Niosh-whc/ https://wwwn.cdc.gov/NIOSH-CEL/ https://wwwn.cdc.gov/eworld https://wwwn.cdc.gov/niosh-mining/ https://wwwn.cdc.gov/niosh-npg https://wwwn.cdc.gov/niosh-oeb https://wwwn.cdc.gov/niosh-ohsn https://wwwn.cdc.gov/niosh-rhd https://wwwn.cdc.gov/PPEINFO/Search https://wwwn.cdc.gov/wisards/ https://wwwn.cdc.gov/wpvhc
40	Does the website have a posted privacy notice?	(•) Yes ( ) No
40a	Is the privacy policy available in a machine-readable format?	(•) Yes ( ) No
41	Does the website use web measurement and customization technology?	(•) Yes ( ) No

Save

		Technologies	Collects PII?
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	○ Yes ○ No
		☐ Web bugs	○ Yes ○ No
		☒ Session Cookies	○ Yes ◉ No
		☒ Persistent Cookies	○ Yes ◉ No
		Other... Omniture: Session Storage via browser	○ Yes ◉ No
42	Does the website have any information or pages directed at children under the age of thirteen?		○ Yes ◉ No
43	Does the website contain links to non-federal government websites external to HHS?		○ Yes ◉ No
General Comments	Q40a: In accordance with HHS's "Rescission of Office of the Chief Information Officer/Superseded Policy for Machine Readable Privacy Policies and Related Guidance Documents" memo. MRPP cannot be validated due to obsolete technology and the suspension of work on P3P by the Platform for Privacy Preferences Project workgroup.		
OPDIV Senior Official for Privacy Signature	Beverly E. Walker -S Digitally signed by Beverly E. Walker -S Date: 2019.08.07 11:52:04 -04'00'		