Save

Privacy Impact Assessment Form

v 1.47.4

Status: Draft | Form Number: F-86426 | Form Date: 3/30/2017 1:15:11 PM

	Question	Answer
1	OPDIV:	CDC
2	PIA Unique Identifier:	P-4278294-258144
2a	Name:	Message Validation, Processing, and Provisioning System (MVPS)
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: Business Steward POC Name: Indira Srinivasan POC Organization: CDC/OPHSS/CSELS POC Email: ibs4@cdc.gov POC Phone: 404-498-6619
7	Is this a new or existing system?	◉ New ○ Existing
8	Does the system have Security Authorization (SA)?	◉ Yes ○ No
8a	Date of Security Authorization	Sep 28, 2018

Save

11	Describe the purpose of the system.	Message Validation, Processing, and Provisioning System (MVPS) is a multifaceted public health disease surveillance system that gives public health officials powerful capabilities to monitor the occurrence and spread of diseases. Facets of MVPS will be used by numerous state, territorial, tribal, and local health departments as well as by partner organizations. The primary goal of MVPS is to develop a common infrastructure for public health agencies that allows the Federal, state, and local level public health agencies to store and exchange data using a common set of business procedures, metadata, and capabilities that can be defined from the start.
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.)	The information stored in the system supports the MVPS mission to monitor the occurrence and spread of diseases by providing data from participating health agencies/providers to be used for disease surveillance by the CDC. The data includes information on patients and patient appointments (e.g., names, mailing address, email addresses, phone numbers, medical notes, date of birth, sex/race, county, marital status and census tract), and the healthcare facilities where the patient appointments occur. External non-CDC users from participating health agencies accessing the system are identified and authenticated via CDC's Secured Access Management System (SAMS), a separate authentication tool with its own Privacy Impact Assessment (PIA). Internal CDC users accessing the system are identified and authenticated via CDC's Active Directory (AD); AD is also a separate system with its own PIA.
13	Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.	The primary goal of the Message Validation, Processing, and Provisioning System (MVPS) is to develop a common infrastructure for public health agencies that allows the Federal, state, and local level public health agencies to store and exchange data using a common set of business procedures, metadata, and capabilities that can be defined from the start and not be introduced ad-hoc. The MVPS system is a message processing system. Messages are received and are then validated. MVPS system data contains information on patients and conditions presented during healthcare visits. This data includes patient name (only for case records with specific conditions); patient mailing address (including county and census tract); patient email address and phone number; medical notes; patient date of birth; and patient gender, race, marital status, and citizenship/nationality. Non-identifiable information collected includes date and time of patient observation, facility information, and case reports on observed conditions. The data is used to associate disease trends among groups like people within a certain age bracket, gender, geographic location, nationality, or race; such information is often of interest to public health officials.

Save

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.	☐ Social Security Number ☒ Date of Birth ☒ Name ☐ Photographic Identifiers ☐ Driver's License Number ☐ Biometric Identifiers ☐ Mother's Maiden Name ☐ Vehicle Identifiers ☒ E-Mail Address ☒ Mailing Address ☒ Phone Numbers ☐ Medical Records Number ☒ Medical Notes ☐ Financial Account Info ☐ Certificates ☐ Legal Documents ☐ Education Records ☐ Device Identifiers ☐ Military Status ☐ Employment Status ☐ Foreign Activities ☐ Passport Number ☐ Taxpayer ID
16	Indicate the categories of individuals about whom PII is collected, maintained or shared.	☒ Employees ☒ Public Citizens ☒ Business Partners/Contacts (Federal, state, local agencies) ☐ Vendors/Suppliers/Contractors ☒ Patients Other
17	How many individuals' PII is in the system?	100,000-999,999
18	For what primary purpose is the PII used?	The PII data is strictly used for research purposes only.
19	Describe the secondary uses for which the PII will be used (e.g. testing, training or research)	PII in the system is used for disease surveillance and reporting. The system needs to be able to associate disease trends among groups like people within a certain age bracket, gender, geographic location, nationality, or race in order to attempt to provide useful information to public health officials.
20	Describe the function of the SSN.	N/A
20a	Cite the **legal authority** to use the SSN.	N/A

Save

21	Identify **legal authorities** governing information use and disclosure specific to the system and program.	Public Health Service Act, Section 301, "Research and Investigation," (42 U.S.C. 241); and Sections 304, 306 and 308(d) which discuss authority to maintain data and provide assurances of confidentiality for health research and related activities (42 U.S.C. 242 b, k, and m(d)).
22	Are records on the system retrieved by one or more PII data elements?	○ Yes ◉ No
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.	0920-0728, Exp. 02/28/2021
24	Is the PII shared with other organizations?	○ Yes ◉ No
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.	No prior notice is given by CDC because MVPS does not collect information directly from any individuals. The actual collection of MVPS data is done by participating state public healthcare agencies. As the original collectors of data, obtaining consent from individuals and notifying individuals about data collection and use are the responsibility of those participating agencies.
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.	The MVPS platform is a "downstream" recipient of data that has already been collected by healthcare agencies at the point of service in their healthcare facilities. Individuals requesting to opt-out must do so according to the policies and procedures in place at those facilities.

Save

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.	The MVPS platform does not have a process to obtain consent from or notify individuals about data collection and use. MVPS is a "downstream" recipient of data that has already been collected by healthcare agencies at the point of service in their healthcare facilities; obtaining consent from and notification of individuals about data use is the responsibility of the agencies that collect it. As a public health authority, the healthcare agencies can exchange the information with CDC to perform health activities without obtaining the individual's consent.
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.	The MVPS system does not have a process in place to work with individuals regarding concerns about their PII stored in the system because the records in the system are not subject to the Privacy Act. Further, consent, notification, and such interactions are conducted between individuals and the healthcare agencies collecting the PII, and are out of scope of the MVPS project and system.
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.	There is an annual review process between the MVPS program and the sending jurisdictions to reconcile and confirm the integrity of case data sent from participating healthcare agencies and data received by the MVPS system. This is conducted with each participating agency at least once every 365 days, and can be done more frequently if a need to do so is determined.
31	Identify who will have access to the PII in the system and the reason why they require access.	☒ Users: Access for data analysis, reporting activities. ☒ Administrators: General access for management of system resources and users. ☐ Developers ☐ Contractors ☐ Others
32	Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	MVPS program management review, on a case-by-case basis, which system users may access PII. The decision is based on the users' job requirements consistent with Role Based Access.
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.	Users are given access according to their jurisdiction and/or program only has access to that information after proofing and approval. The data steward oversees the approval process and determines who gets access to the information for which he or she is responsible. The Least Privilege model is used for all grants of access, and enforced with row-level security in the database.
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 CDC personnel are required to take annual Privacy and Security Awareness Training (SAT).

Save

35	Describe training system users receive (above and beyond general security and privacy awareness training).	All personnel are required to acknowledge HHS Rules of Behavior annually during the SAT.
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.	MVPS data is kept by the CDC as a historical public health record, per CDC's "Scientific and Research Project Records Control Schedule", section 1a ("Authorized Disposition: PERMANENT"). Records Schedule N1-442-09-1.
38	Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.	PII will be secured using a layered approach of Administrative, Technical, and Physical Controls, as follows: Administrative: Users are assigned roles and privileges depending on their job requirements. MVPS program management approves all CDC user access on a case-by-case basis according to the least-privilege principle. MVPS program management also vets and approves access for non-CDC users ("Jurisdictional" Users and Data Managers) also according the principle of least privilege. Technical: MVPS data is protected by restricting access to two points: via CDC's SAMS Authentication platform for external non-CDC users, and via CDC's Active Directory infrastructure for internal CDC users. Once authenticated, users' access to system PII is limited by Role-Based Access Control (RBAC) features built into the MVPS platform. System data is also protected by firewalls, intrusion detection systems, anti-malware systems, and encryption methods provided by CDC's Applied Hosting Branch. Physical Controls: Production and test servers are stored in a server room secured by the CDC. Access tools are in place to secure entry into CDC buildings (Guards, ID Badges, Key Card, Cipher Locks, Closed Circuit TV).

General Comments	
OPDIV Senior Official for Privacy Signature	Beverly E. Walker -S Digitally signed by Beverly E. Walker -S Date: 2018.09.25 16:52:10 -04'00'