

Privacy Impact Assessment Form

v 1.45

Status

Form Number

Form Date

Question

Answer

1 OPDIV:

2 PIA Unique Identifier:

2a Name:

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.

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 POC Name POC Organization POC Email POC Phone

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

<p>11 Describe the purpose of the system.</p>	<p>MVPS system 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; and by partner organizations, such as the Council of State and Territorial Epidemiologists (CSTE).</p> <p>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.</p>	
<p>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.)</p>	<p>Contains patient (case) contact data -Names -mailing address -email addresses, phone numbers, medical notes, DOB, Sex/ Race, county, marital status and census tract</p>	
<p>13 Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.</p>	<p>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.</p> <p>The MVPS system is a message processing system. Messages are received and are then validated.</p> <p>Contains patient (case) contact data; -Names -mailing address -email addresses, phone numbers, medical notes, DOB, Sex/ Race, county, marital status and census tract</p>	
<p>14 Does the system collect, maintain, use or share PII?</p>	<p><input checked="" type="radio"/> Yes <input type="radio"/> No</p>	

15 Indicate the type of PII that the system will collect or maintain.

<input type="checkbox"/> Social Security Number	<input checked="" type="checkbox"/> Date of Birth
<input checked="" type="checkbox"/> Name	<input type="checkbox"/> Photographic Identifiers
<input type="checkbox"/> Driver's License Number	<input type="checkbox"/> Biometric Identifiers
<input type="checkbox"/> Mother's Maiden Name	<input type="checkbox"/> Vehicle Identifiers
<input checked="" type="checkbox"/> E-Mail Address	<input checked="" type="checkbox"/> Mailing Address
<input checked="" type="checkbox"/> Phone Numbers	<input type="checkbox"/> Medical Records Number
<input checked="" type="checkbox"/> Medical Notes	<input type="checkbox"/> Financial Account Info
<input type="checkbox"/> Certificates	<input type="checkbox"/> Legal Documents
<input type="checkbox"/> Education Records	<input type="checkbox"/> Device Identifiers
<input type="checkbox"/> Military Status	<input type="checkbox"/> Employment Status
<input type="checkbox"/> Foreign Activities	<input type="checkbox"/> Passport Number
<input type="checkbox"/> Taxpayer ID	<input type="text" value="County"/>
<input type="text" value="Citizenship/Nationality"/>	<input type="text" value="Census Tract"/>
<input type="text" value="Race/Sex"/>	<input type="text" value="Marital Status"/>

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?

18 For what primary purpose is the PII used?

19 Describe the secondary uses for which the PII will be used (e.g. testing, training or research)

20 Describe the function of the SSN.

20a Cite the **legal authority** to use the SSN.

21 Identify **legal authorities** governing information use and disclosure specific to the system and program.

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:

Published:

Published:

In Progress

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. 01/31/2017

24 Is the PII shared with other organizations?

Yes

No

24a Identify with whom the PII is shared or disclosed and for what purpose.

- Within HHS
- Other Federal Agency/Agencies
- State or Local Agency/Agencies
- Private Sector

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)).

24c Describe the procedures for accounting for disclosures

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.

PII is not collected directly from the individuals. It is collected from the subjects by the state health departments and voluntarily shared with CDC by those state entities in its role as a public health authority.

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.	PII is not collected directly from the individuals. It is collected from the subjects by the state health departments and voluntarily shared with CDC by those state entities in its role as a public health authority.										
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.	PII is not collected directly from the individuals. It is collected from the subjects by the state health departments and voluntarily shared with CDC by those state entities in its role as a public health authority.										
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.	Written notice or electronic notice cannot be given directly to patient or subject as the CDC case notification data does not contain direct personal identifiers (Name, Contact information). All the communication to the patient or subject has to go through the reporting jurisdiction.										
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 for the users that have access to the data. The user data is the responsibility of the jurisdiction. The SAMS data is reviewed within the MISO review process. The source of the the SAMS data is responsible for updating the data. User PII data is verified and synchronized with the source SAMS/MISO systems. Patient PII is currently at rest.										
31	Identify who will have access to the PII in the system and the reason why they require access.	<table border="1"> <tr> <td data-bbox="727 932 951 1024"><input checked="" type="checkbox"/> Users</td> <td data-bbox="951 932 1412 1024">Access for data analysis, reporting activities.</td> </tr> <tr> <td data-bbox="727 1024 951 1117"><input checked="" type="checkbox"/> Administrators</td> <td data-bbox="951 1024 1412 1117">General access for management of system resources and users.</td> </tr> <tr> <td data-bbox="727 1117 951 1188"><input type="checkbox"/> Developers</td> <td data-bbox="951 1117 1412 1188"></td> </tr> <tr> <td data-bbox="727 1188 951 1260"><input type="checkbox"/> Contractors</td> <td data-bbox="951 1188 1412 1260"></td> </tr> <tr> <td data-bbox="727 1260 951 1331"><input type="checkbox"/> Others</td> <td data-bbox="951 1260 1412 1331"></td> </tr> </table>	<input checked="" type="checkbox"/> Users	Access for data analysis, reporting activities.	<input checked="" type="checkbox"/> Administrators	General access for management of system resources and users.	<input type="checkbox"/> Developers		<input type="checkbox"/> Contractors		<input type="checkbox"/> Others	
<input checked="" type="checkbox"/> Users	Access for data analysis, reporting activities.											
<input checked="" type="checkbox"/> Administrators	General access for management of system resources and users.											
<input type="checkbox"/> Developers												
<input type="checkbox"/> Contractors												
<input type="checkbox"/> Others												
32	Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Role Based Access Control (RBAC) is utilized										
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 determine who get access to the information he or she is responsible for. The least Privileged model is used										
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.	Annual Security and Privacy Awareness Training										
35	Describe training system users receive (above and beyond general security and privacy awareness training).	None										

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. Records are retained and disposed of in accordance with the CDC Records Control Schedule. Record copy of study reports are maintained in agency from two to three years in accordance with retention schedules. Source documents for computer are disposed of when no longer needed by program officials. Disposal methods include erasing computer tapes, burning or shredding paper materials or transferring records to the Federal Records Center when no longer needed for evaluation and analysis. Records are retained for 20 years; for longer periods if further study is needed

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. Physical controls are in-place by virtue of the hosting environment. Administrative controls are in-place by virtue of a limited user base (i.e., access is not open). Technical controls are in-place at the application level to grant access to data based on authentication and authorization (e.g., role-based access to jurisdictionally-based data only).

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.

Reviewer Questions

Answer

1 Are the questions on the PIA answered correctly, accurately, and completely? Yes No

Reviewer Notes

2 Does the PIA appropriately communicate the purpose of PII in the system and is the purpose justified by appropriate legal authorities? Yes No

Reviewer Notes

3 Do system owners demonstrate appropriate understanding of the impact of the PII in the system and provide sufficient oversight to employees and contractors? Yes No

Reviewer Notes

4 Does the PIA appropriately describe the PII quality and integrity of the data? Yes No

Reviewer Notes

5 Is this a candidate for PII minimization? Yes No

Reviewer Notes

6 Does the PIA accurately identify data retention procedures and records retention schedules? Yes No

Reviewer Questions		Answer
Reviewer Notes	<input type="text"/>	
7	Are the individuals whose PII is in the system provided appropriate participation?	<input type="radio"/> Yes <input type="radio"/> No
Reviewer Notes	<input type="text"/>	
8	Does the PIA raise any concerns about the security of the PII?	<input type="radio"/> Yes <input type="radio"/> No
Reviewer Notes	<input type="text"/>	
9	Is applicability of the Privacy Act captured correctly and is a SORN published or does it need to be?	<input type="radio"/> Yes <input type="radio"/> No
Reviewer Notes	<input type="text"/>	
10	Is the PII appropriately limited for use internally and with third parties?	<input type="radio"/> Yes <input type="radio"/> No
Reviewer Notes	<input type="text"/>	
11	Does the PIA demonstrate compliance with all Web privacy requirements?	<input type="radio"/> Yes <input type="radio"/> No
Reviewer Notes	<input type="text"/>	
12	Were any changes made to the system because of the completion of this PIA?	<input type="radio"/> Yes <input type="radio"/> No
Reviewer Notes	<input type="text"/>	
General Comments	<input type="text"/>	
OPDIV Senior Official for Privacy Signature	<input type="text"/>	HHS Senior Agency Official for Privacy <input type="text"/>