

Privacy Impact Assessment Form

v 1.47.4

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

8b Planned Date of Security Authorization

 Not Applicable

<p>11 Describe the purpose of the system.</p>	<p>EIP_All Age Hospitalization Database (EIPAAHD) is a population-based network of CDC and state health departments, working with collaborators (local health departments, public health laboratories, clinical laboratories, infection control practitioners, healthcare providers, academic institutions, and other federal agencies) to assess the public health impact of emerging infections and to evaluate methods for their prevention and control. The tool enables users to enter clinical information into data entry screens for inclusion in the CDC Influenza staff's analyses.</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>EIPAAHD maintains information related to patient hospitalization from influenza, for example: information related to enrollment, type of flu test performed, symptoms and vaccination history, and treatment performed. Additional demographics are also collected, such as: Date of Birth (DOB), Hospital name, Hospital admission/discharge date, Nursing Home Resident (Y/N), Age, Sex, Ethnicity and Lab results.</p> <p>External users access the system via the Secured Access Management System (SAMS), a separate access control system. SAMS has its own PIA. Internal users are identified and authenticated via PIV and Active Directory (AD). AD is a separate system with its own PIA.</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 Emerging Infections Programs (EIPs) All Age Hospitalization Database is a population-based network of CDC and state health departments, working with collaborators (local health departments, public health laboratories, clinical laboratories, infection control practitioners, healthcare providers, academic institutions, and other federal agencies) to assess the public health impact of emerging infections and to evaluate methods for their prevention and control. This system allows collection of clinical information for inclusion in the CDC Influenza analyses.</p> <p>EIPAAHD maintains information related to patient hospitalization from influenza, for example: information related to enrollment, type of flu test performed, symptoms and vaccination history, and treatment performed. Additional demographics are also collected, such as: Date of Birth (DOB), Hospital name, Hospital admission/discharge date, Nursing Home Resident (Y/N), Age, Sex, Ethnicity and Lab results. The information related to type of flu test performed, symptoms and vaccination history, and treatment provides insight into cumulative and weekly flu related hospitalizations that are laboratory confirmed cases for flu's weekly publication. No records are extracted by PII and weekly publication only provides aggregated count by categories.</p> <p>External users access the system via the Secured Access Management System (SAMS), a separate access control system. SAMS has its own PIA. Internal users are identified and authenticated via PIV and Active Directory (AD). AD is a separate system with its own PIA.</p>	

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.

<input type="checkbox"/> Social Security Number	<input checked="" type="checkbox"/> Date of Birth
<input 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 type="checkbox"/> E-Mail Address	<input type="checkbox"/> Mailing Address
<input type="checkbox"/> Phone Numbers	<input type="checkbox"/> Medical Records Number
<input 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	

16 Indicate the categories of individuals about whom PII is collected, maintained or shared.

<input type="checkbox"/> Employees
<input type="checkbox"/> Public Citizens
<input type="checkbox"/> Business Partners/Contacts (Federal, state, local agencies)
<input type="checkbox"/> Vendors/Suppliers/Contractors
<input checked="" type="checkbox"/> Patients
Other <input type="text"/>

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

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.

N/A

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.

CDC does not have direct contact with the individuals whose PII is collected. PII is collected by the states and reported to CDC as required by state law. The states have varying processes for notifying individuals.

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.

CDC does not have direct contact with the individuals whose PII is collected. PII is collected by the states and reported to CDC as required by state law. The states have varying processes for notifying individuals.

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.

CDC cannot notify and obtain consent from the individuals whose PII is in the system when major changes occur to the system. PII is collected by the states and reported to CDC as required by state law; however, no PII is reported to that identifies the individuals or provides the ability to contact them.

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.

CDC is not provided PII that directly identifies individuals and hence, has no way of identifying an individual. Thus, CDC cannot validate individual's claim of their data. As all information is collected by the states, redress and grievances can only be addressed by the states.

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.

If a potential inconsistency is detected such as between DOB and hospitalization date, then CDC will request the state to verify the data and retransmit necessary corrections.

31 Identify who will have access to the PII in the system and the reason why they require access.

<input checked="" type="checkbox"/> Users	For data entry and analysis
<input checked="" type="checkbox"/> Administrators	For data management
<input checked="" type="checkbox"/> Developers	For troubleshooting errors
<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.

All users must be approved by the Business Steward (BS) based on roles, duties and responsibilities. Once authorized by the BS, the user will have access to the data. Roles are categorized between read only, and read/write.

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.

AD Role based file and folder permissions limit the user to having either read only or read/write permission to the data.

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.

CDC provides 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. Records are maintained in agency until no longer needed, at which point they will be destroyed. Disposal methods include erasing computer media when no longer needed. 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.

Administrative - users will be granted access on a need to know basis by the Business Owner/Data Manager.
Technical - encryption; AD authentication; Access Control tools.
Physical - The server is hosted in a secure area.

General Comments

Empty text box for general comments.

OPDIV Senior Official
for Privacy Signature