Save

Privacy Impact Assessment Form

v 1.47.2

Status: Draft | Form Number: F-98316 | Form Date: 10/9/2015 1:49:46 PM

	Question	Answer
1	OPDIV:	CDC
2	PIA Unique Identifier:	P-2921661-251279
2a	Name:	BioSense (BioSense)
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: IT Specialist POC Name: Alan Davis POC Organization: CSELS/DHIS/ISB POC Email: ald7@cdc.gov POC Phone: 404-498-6209
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	1/15/2015 12:00:00 AM

Save

11	Describe the purpose of the system.	BioSense is a national syndromic surveillance system funded by the CDC to collect information on emergency departments (EDs) visits and hospitalizations from multiple sources including the Department of Veteran Affairs, the Department of Defense, and civilian hospitals. The BioSense program works in collaboration with participating state and local health departments that have agreed to share data from their own ED monitoring systems to collect information from civilian hospitals. In addition, data from large national labs on tests, orders and results, and pharmaceutical prescription data are included in BioSense. The information will be used nationwide and regionally for situational awareness for all hazard health threats (beyond bioterrorism or early event detection) and to support national, state, and local responses to those threats.
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 data includes location, number of persons involved, symptoms, and outcomes of various disease outbreaks in the nation.
13	Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.	The BioSense program works in collaboration with participating state and local health departments that have agreed to share data from their own ED monitoring systems to
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 age, gender, race, zip code and city of the patient making the visit; and medical information about the visit, including the patient class, chief compliant, triage notes, diagnosis text and codes, patient temperature and pulse

Save

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?	1,000,000 or more
18	For what primary purpose is the PII used?	The Medical Record Number (MRN) is used to assign a "Unique Patient ID" to a patient event record. The Unique Patient ID is then used in forming a "key", the "Unique Visiting ID". The Unique Visiting ID reflects a concatenation of the Facility ID, the Unique Patient ID, and the date (yyyymmdd) of visit. The Unique Visiting ID is used to associate all related messages/records for the same patient event. --- The Date of Birth is currently used in the algorithm applied to establish the "Patient Age". The Patient Age is set by first attempting to calculate the number of years between the Patient Date of Birth, and the Patient Visit Date. If that value cannot be established (e.g., DOB is missing or in incorrect format), then the "Reported Patient Age" that is included in the incoming message is used if not NULL, otherwise the "Calculated Age" that is included in the incoming message is used if not NULL. Note that some local syndromic surveillance reporting laws disallow DOB and others require DOB to be reported. Again our system has to support all possibilities across the range of public health departments in the country. --- The Chief Complaint is used in algorithms that parse the text and categorize the Chief Complaint into one or more syndromic categories of interest. These syndromic categories, also known as "bins" total over 100 categories including "Fever", "Influenza like illness", "Injury", etc... A patient event may be reflected in multiple messages/records for the same person/same event, and may have Chief Complaint(s) that match one or more syndromic categories. The system leverages the Unique Visiting ID to associate the syndromic categories with the same patient event. These data are then use in statistical algorithms to produce signals should the data reveal an unusual spike in one or more syndromic categories.

Save

19	Describe the secondary uses for which the PII will be used (e.g. testing, training or research)	The MRN can be used to crosswalk patient events with multiple visit numbers. It is recommended that data providers submit the patient medical record number to facilitate identification of the patient, in the event of a required follow-up investigation. This is a function supported for local health departments who are using our system as their primary system. It is not for CDC to use in this manner without expressly being asked to do so in order to assist the local health department. Without the medical record number, the work required to follow-up on the records of interest greatly increases on the data provider and may cause unacceptable delays in public health response. In addition, the medical record number may aid in record de-duplication efforts and may often aid in the resolution of apparent transcription errors. --------- The Date of Birth can be used in data quality assurance checks. For example, the Date of Birth for multiple visit records containing the same Unique Patient ID should be static. Additionally, the Date of Birth can be used to assess accuracy of other alternate data elements containing Age such as the reported age and calculated age are sometimes updated to reflect the patient's current age, and not the age at the time of event. This may happen if update messages are sent in for a patient event that took place in the past, where the age sent in the update reflects the current age and not the age at the time of the event. That said, some areas are prohibited to send date of birth and rely on including the reported and/or calculated age in the incoming message. ---------- The Chief Complaint can be used to search for specific terms or combination of terms. This is especially useful if the current rules do not cover a specific category of interest. It is important to note that this is really the life blood of syndromic surveillance and provides the most value – the ability to near real time assess new and unusual events of interest. In addition, the Chief Complaint can be used to apply quality assurance checks to existing binning rules to verify the rules are yielding the correct categories based on the original text found in the Chief Complaint. Related, similar quality assurance checks can be applied as new syndromic definitions are developed. The Chief Complaint can also be used to check the content of messages in new feeds during the onboarding process to insure the data reflect patients' chief complaints and not a standard term such as "ER visit" that does not contain sufficient information to categorize the visit into appropriate syndromic categories.
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.	PHSA Section 306; Public Health Security and Bioterrorism Preparedness and Response Act of 2002; and the Pandemic and All-Hazards Preparedness Reauthorization Act of 2013
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: 09-20-0136 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.	0920-0824, 11/30/2015
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 The data will be used for situational awareness for all-hazard health threats (beyond bioterrorism or early event detection) and to support national, state, and local responses to those threats. ☒ State or Local Agency/Agencies The data will be used for situational awareness for all-hazard health threats (beyond bioterrorism or early event detection) and to support national, state, and local responses to those threats. ☐ 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)).	BioSense requires data use agreements (DUAs) with all providers that govern the retention and destruction of PII. The DUAs provide guidance and agreement on areas including sole use by the data source in a secure space, shared space, other health agency uses, and maintaining and disposing of data in a distributed computing environment and all policies and applicable procedures in compliance with the Federal Information Security Management Act (FISMA).
24c	Describe the procedures for accounting for disclosures	Any disclosure will be documented in a log maintain by the program. The log will include who the information was disclosed to, when the the disclosure was made, and when the request for disclosure was received.
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.	BioSense does not collect information directly from individuals. The submission of PII to the system by contributing agencies is voluntary. The participating agencies are the original collector and maintainer of data, so any notifications would be handled by contributing institutions.
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 submission of PII by contributing agencies is voluntary. The participating agencies are the original collector and maintainer of data, granting secondary access to BioSense users. BioSense does not collect information directly from individuals. The option to opt-out, if any, would be handled by the participating agencies.
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 collection of PII conducted by BioSense partners falls within the HIPAA exemption for public health institutions; thereby removing the necessity for individual consent. BioSense is a secondary user of data and does not conduct any primary data collection.

Save

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.	BioSense does not collect data direct from individuals. The contributing institutional partners collect data. All PII issues and concerns are addressed by the contributing partners.	
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.	The program will perform annual internal system audits to review the PII collected. This review will focus on ensuring the data's accuracy and integrity, and that the data is being received in accordance with the Public Health Information Network (PHIN) guide.	
31	Identify who will have access to the PII in the system and the reason why they require access.	☒ Users	By using shared data from multiple jurisdictions (shared per fully executed data-use agreements), state and local health departments, and federal agencies can put together regional and national pictures routinely or during events. Users can create views and set alert thresholds to look at only the particular information that is of interest or utility to them.
		☒ Administrators	Administrators are required to have access to the database to maintain the system.
		☒ Developers	Developers are required to have access to the database to maintain the system, provide further development, and maintain the data.
		☒ Contractors	ICF is the contractor charged with running the system and maintaining the Data.
		☐ Others	
32	Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Requests for access to this data are reviewed and approved by officials from the jurisdiction which supplied the data to CDC. If the access request is approved, either the BioSense system makes the data available automatically, or the BioSense contractor implements the necessary permissions within the system to grant access. Users with a need to access these data will submit a written request to the BioSense contractor via the technical support website. Requests are reviewed and approved by CDC officials and officials from the jurisdiction which supplied the data to CDC. If the access request is approved, the BioSense contractor implements the necessary permissions within the system to grant 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 assigned roles based on their need to access data and the system. Password protection is enforced for different roles and levels specific to job responsibility.	

Save

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.	Each user of the system is required to read and acknowledge the rules of conduct located at https://www.biosen.se/login.php. Users are notified of this review and must acknowledge annually.
35	Describe training system users receive (above and beyond general security and privacy awareness training).	N/A
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.	Input Data (Electronic feed(s) from other electronic systems)/ Dispose when data no longer needed. System Data (created for research purposes that may be required for follow up or reference for a moderate period of time)/ Maintain at least six years, but no longer than ten years after the retirement of the system depending upon program need for scientific, legal, or business reference then delete/ destroy. Output Data (Final reports: In summary form, the findings and conclusions reached relative to scientific projects both with CDC and through Contractual arrangements/Permanent. Output Data (Reference copies: test runs, data corrections, daily operational documents, for example)/Dispose when no longer needed. Output Data (Substantive reporting material)/Permanent. Output Data (Routine reporting material)/Five years. Output Data (Printouts derived from electronic records created on an ad-hoc basis for reference purposes or to meet day-today business needs/Dispose when no longer needed.
38	Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.	CDC users must use PIV authentication. Other users are required to have a user name and strong password. The system environment is monitored via daily server logs which support the system's continuous monitoring strategy. BioSense uses Logwatch to notify the project if unauthorized remote connections are attempted. BioSense also uses Amazon Web Services AWS Identity and Access Management (IAM) to securely control access to AWS services and resources for users.

General Comments	

OPDIV Senior Official for Privacy Signature	Beverly E. Walker -S Digitally signed by Beverly E. Walker -S Date: 2015.10.20 13:27:47 -04'00'	HHS Senior Agency Official for Privacy	