Archived Privacy Impact Assessment (PIA): CDC - BioSense - QTR3 - 2023 - CDC6798524

Created Date: 7/20/2023 12:05 PM Last Updated: 2/13/2025 10:47 AM

Copy PIA (Privacy Impact Assessment)

Do you want to copy this PIA ?

Please select the user, who would be submitting the copied PIA.

Instructions

Review the following steps to complete this questionnaire:

1) Answer questions. Select the appropriate answer to each question. Question specific help text may be available via the icon. If your answer dictates an explanation, a required text box will become available for you to add further information.

2) Add Comments. You may add question specific comments or attach supporting evidence for your answers by clicking on the icon next to each question. Once you have saved the comment, the icon will change to the icon to show that a comment has been added.

3) Change the Status. You may keep the questionnaire in the "In Process" status until you are ready to submit it for review. When you have completed the assessment, change the Submission Status to "Submitted". This will route the assessment to the proper reviewer. Please note that all values list questions must be answered before submitting the questionnaire.

4) Save/Exit the Questionnaire. You may use any of the four buttons at the top and bottom of the screen to save or exit the questionnaire. The button allows you to complete the questionnaire. The button allows you to save your work and close the questionnaire. The button allows you to save your work and remain in the questionnaire. The button closes the questionnaire without saving your work.

Acronyms

ATO - Authorization to Operate
CAC - Common Access Card
FISMA - Federal Information Security Management Act
ISA - Information Sharing Agreement
HHS - Department of Health and Human Services
MOU - Memorandum of Understanding
NARA - National Archives and Record Administration
OMB - Office of Management and Budget
PIA - Privacy Impact Assessment
PII - Personally Identifiable Information
POC - Point of Contact
PTA - Privacy Threshold Assessment
SORN - System of Records Notice
SSN - Social Security Number
URL - Uniform Resource Locator

Does this need to migrate to a Sub-Component?:

Consolidated Parent Component

Component Name
No Records Found

General Information

PIA Name:	CDC - BioSense - QTR3 - 2023 - CDC6798524	**PIA ID:**	6798524
Name of Component:	BioSense	**Name of ATO Boundary:**	BioSense

Migrated Sub-Component PIA

PIA Name
No Records Found

Sub-Component

Software Name
No Records Found

Original Related PIA ID

PIA Name
No Records Found

Overall Status:		**PIA Queue:**	
Submitter:	BLACKBURN, Jason	**# Days Open:**	405
Submission Status:	Re-Submitted	**Submit Date:**	7/30/2024
Next Assessment Date:	08/28/2027	**Expiration Date:**	8/28/2027
Office:	DDPHSS	**OpDiv:**	CDC
Security Categorization:	Moderate		
Legacy PIA ID:		**Make PIA available to Public?:**	Yes
1:	Identify the Enterprise Performance Lifecycle Phase of the system		
2:	Is this a FISMA-Reportable system?		
3:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?		
4:	ATO Date or Planned ATO Date		9/30/2024

Privacy Threshold Analysis (PTA)

PTA Name
CDC - BioSense - QTR2 - 2023 - CDC6785120

History Log:	View History Log

PTA

PTA

PTA - 2:	Indicate the following reason(s) for this PTA. Choose from the following options.	PIA Validation (PIA Refresh)
PTA - 2A:	Describe in further detail any changes to the system that have occurred since the last PIA.	N/A - No changes to the function of the system overall, the constituencies served, or the data contained within the system
PTA - 3:	Is the data contained in the system owned by the agency or contractor?	Agency

PTA - 4:	Please give a brief overview and purpose of the system by describing what the functions of the system are and how the system carries out those functions.	The BioSense platform is an interactive partnership between the CDC and the public health community, contributing to the CDC's public health mission by tracking health hazards in the United States as they evolve (i.e. - syndromic surveillance). The BioSense platform helps automate public health syndromic surveillance data collection and provides timely public health information. BioSense provides public health officials at all levels with the data, information, and tools they need to make better decisions about how to protect and improve the health of all people.
PTA - 5:	List and/or describe all the types of information that are collected (into), maintained, and/or shared in the system regardless of whether that information is PII and how long that information is stored.	The data in the Biosense Platform is the Emergency Room Data ("ED") data provided by the system's "jurisdictions", which are mostly state health systems, although the Biosense Platform does receive data collected by the Department of Defense (DoD) ,US Department of Veterans Affairs (VA), and by Labcorp, a commercial medical testing lab. ED data typically includes the facility identification, the time of the patient visit, patient age (month and year only), gender, race, symptoms presented, and other data about the condition of the patient; the data is kept by the CDC as a historical public health record. It is important to note that the Biosense Platform is not considered to "collect" the data itself, but receives it from the entities described above. The medical data consists of patient visit information with a particular focus on the condition presented (cold, flu, etc.), location and date/time of the patient visit. Minimal PII (patient Year of Birth and Month of Birth and medical notes) are also included. The actual Day of Birth is not included. For internal CDC users, access is via CDC's Personal Identity Verification (PIV)-compliant Active Directory Network infrastructure, so no userID's or passwords are stored in the system. Active Directory is a separate tool with its own PIA. External users authenticate via userIDs and passwords, which are deleted from the system when no longer needed.
PTA - 5A:	Are user credentials used to access the system?	
PTA - 5B:	Please identify the type of user credentials used to access the system.	Non-HHS User Credentials Username Password HHS User Credentials HHS/OpDiv PIV Card

PTA - 6:	Describe why all types of information is collected (into), maintained, and/or shared with another system. This description should specify what information is collected about each category of individual.	The data in the Biosense Platform is the Emergency Room Data ("ED") data provided by the system's "jurisdictions", which are state health systems, the Department of Defense (DoD) ,US Department of Veterans Affairs (VA), and by Labcorp, a commercial medical testing lab. The data is owned by the participating jurisdictional partners. ED data typically includes the facility identification, the time of the patient visit, patient age (month and year only), gender, race, symptoms presented, tests performed (if any), and other data about the condition of the patient; the data is kept by the CDC as a historical public health record." The PII data collected per each test/ED visit are DOB (Year + Month) to assess the patient's age Medical Notes are collected if a particular case requires follow-up. It is important to note that the Biosense Platform is not considered to "collect" the data itself, but receives it from the entities described above. The medical data consists of patient visit information with a particular focus on the condition presented (cold, flu, etc.), location and date/time of the patient visit. Data is collected to support BioSense as a national syndromic surveillance system funded by the CDC to collect information on emergency departments (EDs) visits and hospitalizations. 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. By using shared surveillance data from multiple jurisdictions (shared per fully executed data use agreements), partners such as federal, academic, commercial, state and local health departments can put together regional and national picture of situational awareness routinely or during significant events.
PTA - 7:	Does the system collect, maintain, use or share PII?	Yes
PTA - 7A:	Does this include Sensitive PII as defined by HHS?	No
PTA - 8:	Does the system include a website or online application?	Yes
PTA - 8A:	Are any of the URLs listed accessible by the general public (to include publicly accessible log in and internet websites/online applications)?	No
PTA - 9:	Describe the purpose of the website, who has access to it, and how users access the web site (via public URL, log in, etc.). Please address each element in your response.	Two reporting applications (ESSENCE and RStudIo) are accessed by Biosense users. External partners include members of State & Local health systems, Federal (Veterans Administration),

PTA - 10:	Does the website have a posted privacy notice?	Yes
PTA - 11:	Does the website contain links to non-federal government websites external to HHS?	No
PTA - 11A:	Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?	
PTA - 12:	Does the website use web measurement and customization technology?	No
PTA - 12A:	Select the type(s) of website measurement and customization technologies in use and if it is used to collect PII.	
PTA - 13:	Does the website have any information or pages directed at children under the age of thirteen?	No
PTA - 13A:	Does the website collect PII from children under the age thirteen?	
PTA - 13B:	Is there a unique privacy policy for the website and does the unique privacy policy address the process for obtaining parental consent if any information is collected?	
PTA - 14:	Does the system have a mobile application?	No
PTA - 14A:	Is the mobile application HHS developed and managed or a third-party application?	
PTA - 15:	Describe the purpose of the mobile application, who has access to it, and how users access it. Please address each element in your response.	
PTA - 16:	Does the mobile application/ have a privacy notice?	
PTA - 17:	Does the mobile application contain links to non-federal government website external to HHS?	
PTA - 17A:	Is a disclaimer notice provided to users that follow external links to resources not owned or operated by HHS?	
PTA - 18:	Does the mobile application use measurement and customization technology?	
PTA - 18A:	Describe the type(s) of measurement and customization technologies or techniques in use and what information is collected.	
PTA - 19:	Does the mobile application have any information or pages directed at children under the age of thirteen?	
PTA - 19A:	Does the mobile application collect PII from children under the age thirteen?	
PTA - 19B:	Is there a unique privacy policy for the mobile application and does the unique privacy policy address the process for obtaining parental consent if any information is collected?	
PTA - 20:	Is there a third-party website or application (TPWA) associated with the system?	No
PTA - 21:	Does this system use artificial intelligence (AI) tools or technologies?	No

PIA

PIA

PIA - 1:	Indicate the type(s) of personally identifiable information (PII) that the system will collect, maintain, or share.	Date of Birth Medical Records Number Other - Free text Field - Medical notes, gender, race.
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared.	Patients
PIA - 3:	Indicate the approximate number of individuals whose PII is maintained in the system.	Above 2000

PIA - 4:	For what primary purpose is the PII used?	PII MRN and DOB (mm/yy) is used by jurisdictional partners (prior to making data available to the Biosense platform) to create a unique key value to associate all related messages/records for the same patient event (appointment, Emergency Room visit, etc.) to tie the various records generated during the patient event together in, which then becomes the foundational data upon which the Biosense Platform's summarized geotracking of disease outbreaks and prevalence is based. MRN is not sent to or stored in Biosense. Note: Individuals can not be identified by the Biosense system as the Medical Record Numbers (MRNs) are transformed, by the contributing agency prior to the data being made available to the Biosense platform, to protect patient privacy. As mentioned, the MRNs are not sent to Biosense by contributing jurisdictions.
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	The Month & Year of birth can be used in data quality assurance checks (note - the system does not receive the complete DOB - the day of birth is not included in the data from participating jurisdictions). 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. Medical Notes 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, Medical Notes 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 Medical Notes. Related, similar quality assurance checks can be applied as new syndromic definitions are developed. Medical Notes 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.
PIA - 6:	Describe the function of the SSN and/or Taxpayer ID.	N/A

PIA - 6A:	Cite the legal authority to use the SSN.	N/A
PIA - 7:	Identify legal authorities, governing information use and disclosure specific to the system and program.	Biosense operates under: Public Health Service Act, Section 301, Research and Investigation," (42 USC 241); and Sections 304, 306, and 308(d) which discuss authority to maintain data and provide assurances of confidentiality for health research ad related activities; and Sec. 103. "Improving ability of Centers for Disease Control and Prevention" of the Public Health Security and Bioterrorism Preparedness and Response Act of 2002; and the Pandemic and All-Hazards Preparedness Reauthorization Act of 2013; under which the CDC developed and modified the BioSense Program to establish and maintain an integrated system of nationwide public health surveillance for the early detection and prompt assessment of potential bioterrorism-related illness.
PIA - 8:	Are records in the system retrieved by one or more PII data elements?	No
PIA - 8A:	Please specify which PII data elements are used to retrieve records.	
PIA - 8B:	Provide the number, title, and URL of the Privacy Act System of Records Notice (SORN) that is being used to cover the system or indicate whether a new or revised SORN is in development.	
PIA - 9:	Identify the sources of PII in the system.	Government Sources State/Local/Tribal Other Federal Entities Non-Government Sources Members of the Public
PIA - 10:	Is there an Office of Management and Budget (OMB) information collection approval number?	Yes
PIA - 10A:	Provide the information collection approval number.	0920-0824
PIA - 10B:	Identify the OMB information collection approval number expiration date.	3/31/2026
PIA - 10C:	Explain why an OMB information collection approval number is not required.	N/A - see PIA - 10A. There is an OMB number
PIA - 11:	Is the PII shared with other organizations outside the system's Operating Division?	Yes
PIA - 11A:	Identify with whom the PII is shared or disclosed.	Other Federal Agency/Agencies State or Local Agency/Agencies

PIA - 11B:	Please provide the purpose(s) for the disclosures described in PIA - 11A.	BioSense platform features data use agreements (DUAs) data between state health agencies and CDC governing use of data including PII in compliance with the Federal Information Security Management Act (FISMA). For example, CDC and Veterans Health Administration share a MOU; the VHA's nationwide scope contributes to CDC's ability to conduct disease surveillance covered by the Public Health Service Act. The MOU outlines the rules for the CDC to analyze, use to develop methods, share with other governmental health agencies the event-level data, and also lists the rules governing use of data (to public health officials in connection with the purpose of the research) & settlement of disputes Center for Disease Control Biosense Data Sharing Memorandum of Agreement with the Defense Health Agency outlines the requirements of the Public Health Security and Bioterrorism Preparedness and Response Act of 2002. The agreement also outlines the interface method and the specific responsibilities of each entity with respect to meeting DoD safeguards, protection from viruses and malicious code, physical security, integrity and auditability.
PIA - 11C:	List any agreements in place that authorize the information sharing or disclosure (e.g., Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or Information Sharing Agreement (ISA)).	• NSSP Data Use Agreements(2012,2015,2018,2021) - 67 sites • Veterans Health Administration Memorandum of Understanding (2020) • Defense Healthcare Management (DHA) Memorandum of Agreement (2020) • Labcorp Memorandum of Understanding (2018) • In- Draft Still: CDC Common Agreement and NSSP Addendum D (2024) – 0 sites
PIA - 11D:	Describe process and procedures for logging/tracking/accounting for the sharing and/or disclosing of PII. If no process or procedures are in place, please explain why not.	Biosense information is not "disclosed" to other entities; other Healthcare agencies participating in the Biosense system (i.e. - "jurisdictions") are able to access the Biosense system, but they can only access their own data or data from other jurisdictions with whom they have data sharing agreements. Given that, there are no specific accounting procedures for information disclosures for the Biosense program.
PIA - 12:	Is the submission of PII by individuals voluntary or mandatory?	Voluntary
PIA - 12A:	If PII submission is mandatory, provide the specific legal requirement that requires individuals to provide information or face potential civil or criminal penalties.	

PIA - 13:	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 Biosense platform is a "downstream" recipient of data that has already been collected by state health agencies from their instate health facilities; individuals requesting to opt-out must do so with the facility they are patients of. The opt-out process is out of scope of the Biosense project and system. The submission of PII by contributing agencies is covered under Public Health Security and Bioterrorism Preparedness and Response Act of 2002.
PIA - 14:	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.	Individuals can not be identified by the Biosense system as the Medical Record Numbers (MRNs) are transformed, by the contributing agency prior to the data being made available to the Biosense platform, to protect patient privacy. The MRNs are not stored in the Biosense system.
PIA - 15:	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 from individuals and can not identify individuals. The contributing jurisdictional partners collect data. All PII issues and concerns are addressed by the contributing partners (state health agencies, the Department of Defense, and the Veterans Administration).
PIA - 16:	Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy. Please address each element in your response. If no processes are in place, explain why not.	BioSense maintains a security configuration checklist that defines mandatory settings for security related parameters. Any unauthorized changes to these configurations are tracked, monitored, and logged to support incident response. Additionally, system data is scanned weekly to ensure that participating jurisdictions are not transmitting prohibited PII (patient name, address, complete date of birth, identifying numbers, etc.). Facilities identified as sending that information are blocked from further transmission, and records with that information are deleted. Once the sending jurisdictions have corrected the issue, their data is allowed back into the system.
PIA - 17:	Identify who will have access to the PII in the system.	Users Administrators Developers Contractors
PIA - 17A:	Select the type of contractor.	HHS/OpDiv Direct Contractors
PIA - 17B:	Do contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices?	Yes

PIA - 18:	Provide the reason why each of the groups identified in PIA - 17 needs access to PII.	**Administrators** — As part of their job responsibility to set-up, configure, and maintain the information systems making up the BioSense Platform, system administrators may potentially need to access any file on the information system. This necessarily includes files that may contain PII. System administrators may be tasked with auditing files or logs for potential PII or other sensitive information. Should PII be discovered, system administrators may be tasked with protecting the file from access by other users, with securely erasing the data, or directing the sensitive information into an appropriate storage and processing pipeline. **Developers** — While most development work occurs in an isolated development environment using test data, some development and testing must necessarily be performed in a production environment using live data. In some circumstances, this may involve the developer having access to PII data elements in order to correctly design, implement, and deploy their code. For example, a scanner module was developed to detect and redact telephone numbers that were entered into the chief complaint text without removing important syndromic surveillance information from the same data element. While the developer could and did build the module without access to live data, the developer was also a member of the team that was responsible for verifying the correct operation of the module when it was placed into production. This necessarily involves viewing pre- and post-redaction chief complaint data, with the pre-redaction data including PII. **Contractors** — CDC uses contractors to develop and administer the BioSense platform. Contractors assigned to the administrator role require the same level of access, including to PII, as any other system administrator. Contractors assigned to the developer role require the same level of access as any other developer, which again may involve access to PII depending on the specific development tasks being performed. **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.

PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Access to the system and data is granted on a case-by-case basis by Biosense program management based on the principle of least privilege. CDC users are granted access to data for operational support purposes only and have access to data from all sources. Non-CDC end users may only obtain access to their jurisdiction's data via their jurisdiction's data steward's written permission provided to the CDC.
PIA - 20:	Describe the technical 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. The least Privileged model is used.
PIA - 21:	Identify the general security and privacy awareness training provided to system users (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 embedded in the Access and Management Center ("AMC") before system access is enabled. Every 90 days when AMC and ESSENCE (ESSENCE is a software package) passwords must be changed, users are required to read and acknowledge the BioSense Platform Code of Conduct. Additionally, HHS Rules of Behavior and Security Awareness training provides training for personnel using the system to make them aware of their responsibilities for protecting the information being collected and maintained.
PIA - 22:	Describe training system users receive (above and beyond general security and privacy awareness training).	None
PIA - 23:	Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific National Archives and Records Administration (NARA) records retention schedule(s) and include the retention period(s).	The Data Use Agreements (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). Records are retained indefinitely until no longer needed, per CDC's "Scientific and Research Project Records Control Schedule", section 1a ("Authorized Disposition: PERMANENT"), N1-442-2009-01. Note: contributing jurisdictions own their own data and can delete it at any time.

PIA - 24:	Describe how the PII will be secured in the system using administrative, technical, and physical controls. Please address each element in your response.	Biosense' administrative, technical, and physical security controls present a layered approach that are based on National Institute of Standards and Technology (NIST) SP 800-53 as required to operate at the Federal Information Security and Management Act (FISMA)-Moderate level (p.17, SSP). **Physical controls:** Biosense data is protected by physical controls including physical barriers and locked doors protecting restricted areas, guards, video cameras, climate control (cooling), redundant power systems, and fire prevention and control systems. **Technical controls:** Biosense' technical controls include Role-Based Access Control for all users (system administrators, developers, and users), encryption, multiple firewalls, and system redundancy. The system also undergoes continuous monitoring using automated monitoring systems. **Administrative controls:** Biosense' administrative controls include restricted access to the system; each individual user is vetted by Biosense program management. Security Awareness Training is required and must be updated annually. Background checks are required for all users. OMB (Office of Management and Budget), HHS and CDC security and privacy policies and standards are followed by all users of the system.

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	**Privacy Analyst Review Date:**	7/30/2024
Privacy Analyst Comments:	OpDiv Analyst: Joshua Mosios (Contractor)	**Privacy Analyst Days Open:**	

SOP Review

SOP Review Status:	Approved	**SOP Signature:**	JWO Signature.docx
SOP Comments:	Approved on behalf of Beverly Walker	**SOP Review Date:**	8/5/2024
		SOP Days Open:	6

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	8/9/2024
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte 8/9/2024 This PIA is ready for SAOP review and approval.	**Agency Privacy Analyst Days Open:**	4

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	
SAOP Comments:		**SAOP Review Date:**	8/28/2024
		SAOP Days Open:	19

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
No Records Found				

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 1	MOSIOS, Joshua	6/6/2024	Pleases include "medical notes" and demographic information such as gender and race.	
PIA - 9	MOSIOS, Joshua	6/6/2024	Please select "members of the public"	
PIA - 11B	OSHODI, Jarell	7/1/2024	Has ASTHO been defined?	
PIA - 18	OSHODI, Jarell	7/2/2024	Provide descriptions with 4 different paragraphs for each named group.	
PIA - 11C	Data Feed Service, Sync2PIAForm	8/8/2024	Please remove the bullet points for 508 compliance.	
PIA - 11B	Data Feed Service, Sync2PIAForm	8/8/2024	Please write out "MOU" in the first instance.	