Privacy Impact Assessment (PIA): CDC - NVDRS Web - QTR2 - 2023 - CDC6736129

Created Date: 4/25/2023 2:01 PM Last Updated: 11/22/2023 1:40 PM

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 - NVDRS Web - QTR2 - 2023 - CDC6736129	**PIA ID:**	6736129
Name of Component:	National Violent Death Reporting System Web Enablement	**Name of ATO Boundary:**	National Violent Death Reporting System Web Enablement

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:	PATEL, Anusha	**# Days Open:**	94
Submission Status:	Re-Submitted	**Submit Date:**	5/9/2023
Next Assessment Date:	07/27/2026	**Expiration Date:**	7/27/2026
Office:	NCIPC	**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	7/31/2023

Privacy Threshold Analysis (PTA)

PTA Name
CDC - NVDRS Web - QTR1 - 2023 - CDC6695197

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.	Migrating from on-premises to the OCIO managed Azure Cloud. No changes to functionality.
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 National Violent Death Reporting System (NVDRS) is an incident-based system designed to capture data on violent deaths (suicides, homicides, deaths of undetermined intent, and unintentional firearm deaths) in a relational database. This system allows data from law enforcement reports, death certificates, and coroner/medical examiner reports to be combined into one cohesive data base allowing a variety of public health professionals and decision-makers to analyze and understand the nature of and trends of violence in the United States. NVDRS is the only state-based surveillance (reporting) system that pools data on violent deaths from multiple sources into a usable, anonymous database.
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.	NVDRS Web collects homicide, suicide, unintentional firearm injury, and unintentional drug overdose decedents data. The information may be grouped as follows: demographics, including age, race, ethnicity, industry and occupation, military service, area of residence, height, weight, level of education; Injury and Death, including number and location of wounds, underlying and contributing causes of death, date and time of injury and death, type of location where injured, provision of medical treatment prior to death, survival time; Circumstances attending the incident, such life stressors, contributing medical or psychological conditions, precipitating circumstances such as arguments or crimes in progress; Number and type of weapons involved in the incident; relationship between the decedent and any suspect(s) in the case of homicide; Toxicological information collected from the decedent. There are over 700 data elements in collected in NVDRS, as detailed in the NVDRS Coding Manual, available at: https://www.cdc.gov/violenceprevention/datasources/nvdrs/resources.html. All information is stored for the duration of the program, which has no planned termination date.
PTA - 5A:	Are user credentials used to access the system?	
PTA - 5B:	Please identify the type of user credentials used to access the system.	
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.	NVDRS captures data on violent deaths (suicides, homicides, deaths of undetermined intent, and unintentional firearm deaths) to promote greater functionality and improved access to data that inform the development, implementation, and evaluation of violence prevention strategies. There are no interconnections with other systems. NVDRS does not update, maintain, or share information with other systems.
PTA - 7:	Does the system collect, maintain, use or share PII?	Yes
PTA - 7A:	Does this include Sensitive PII as defined by HHS?	Yes
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.	**https://sams.cdc.gov** Identity verification and access to NVDRS Web is controlled by the SAMS platform. External users log in with username and password via SAMS and Internal users authenticate using PIV credentials via SAMS. **https://nvdrs.cdc.gov/** The NVDRS Web website is used by grantees to abstract cases into the database, review and correct information, and perform basic quality checks on the data entered. A Principal Investigator in each grantee state or territory identifies users that should have access to the system. Access is limited only to those who have been identity verified and authenticated via SAMS. Users only have access to records for their particular state or territory.
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?	Yes
PTA - 12A:	Select the type(s) of website measurement and customization technologies in use and if it is used to collect PII.	Session Cookies - Does Not 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?	No
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.	Other - Free text Field - The combination of the follo Incident year Incident state Incident number The combination of two or more of the following fiel Year of incident State of incident Incident number Incident type Case status Flag for follow-up Victim's age Victim's sex First initial of victim's last name Date of death ZIP Code of injury ZIP Code of residence Victim's day of birth & month (ex. 1-31) Last four digits of victim's Coroner/Med Last four digits of victim's Death Certific
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared.	Patients Members of the public
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?	There are no individual PII data elements in NVDRS Web and patients' complete medical records are not available in this system. However, the combination of two or more non-sensitive data elements in NVDRS Web can make a probabilistic or an exact match to an incident or deceased individual, and therefore treated as PII. The NVDRS Web is an incident-based system designed to capture data on violent deaths (suicides, homicides, deaths of undetermined intent, and unintentional firearm deaths) in a relational database. NVDRS promotes greater functionality and improved access to data that inform the development, implementation, and evaluation of violence prevention strategies. NVDRS increases knowledge about where violent deaths occur, who is most at risk, and the factors that contribute to violent deaths. These data provide the foundation for building successful strategies for preventing violence so that all communities are safe and free from violence and people can live to their full potential.
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	There are no secondary uses for NVDRS Web data.
PIA - 6:	Describe the function of the SSN and/or Taxpayer ID.	N/A - NVDRS Web does not collect, maintain, or disseminate SSN and/or Taxpayer ID.
PIA - 6A:	Cite the legal authority to use the SSN.	N/A - NVDRS Web does not collect, maintain, or disseminate SSN and/or Taxpayer ID.
PIA - 7:	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)
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.	OMB Approval Number 0920-0607
PIA - 10B:	Identify the OMB information collection approval number expiration date.	9/30/2025
PIA - 10C:	Explain why an OMB information collection approval number is not required.	OMB information collection approval number is required and provided above.

PIA - 11:	Is the PII shared with other organizations outside the system's Operating Division?	No
PIA - 11A:	Identify with whom the PII is shared or disclosed.	
PIA - 11B:	Please provide the purpose(s) for the disclosures described in PIA - 11A.	
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)).	
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.	
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.	N/A - NVDRS Web data elements pertain to deceased individuals, so the opt-out method does not apply.
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.	N/A - NVDRS Web data elements pertain to deceased individuals, so notification and consent is not possible.
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.	N/A - NVDRS Web data elements pertain to deceased individuals, so resolving deceased individuals' concerns is not possible. However, if there is a concern that a living person may have regarding the deceased individual's data, then they should contact ncipcitsecurity@cdc.gov.
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.	System and Security Stewards review NVDRS Web data elements contained in the system annually (every 365 days), concurrent with resubmission of the system Privacy Impact Assessment (PIA) and review of the Baseline System Information (BSI). NVDRS undergoes at least one enhancement effort each 365 days, during which the integrity, availability and relevancy of the entire data dictionary are assessed and updated according to program needs. NVDRS Web also requires that state-level partner agencies revalidate their NVDRS records within every 365 days.
PIA - 17:	Identify who will have access to the PII in the system.	Users Administrators
PIA - 17A:	Select the type of contractor.	
PIA - 17B:	Do contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices?	

PIA - 18:	Provide the reason why each of the groups identified in PIA - 17 needs access to PII.	Users Information on deaths is collected by state-level partner agencies (typically state health departments), and information is transmitted to the CDC after being stripped of all personally identifiable information (PII). Each state's own Violent Death Reporting System establishes the details of that state's cases from primary and secondary data sources. Administrators Administrators need access to data to administer and provide system support. There are no PII elements in the system, only non-sensitive data that if combined could make a probabilistic or an exact match to an incident or deceased individual.
PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	The least privilege model will be used to allow those with access to NVDRs Web data elements to be able to access the minimum amount of information needed. Users are only granted access to specific files needed to perform their job. No one is granted more access than is necessary. NVDRS State User – An individual who has been invited on behalf of a SAMS protected 'client' application and successfully completed the SAMS Partner Portal registration process, all required identity verification steps, and who has been authorized to access at least one (1) NVDRS SAMS-protected activity. - Users may be State government workers, contractors or interns - Have permission limited to searching and entering/editing violent death data and viewing reports for their assigned state. NVDRS State Administrator – An individual who has been invited on behalf of a SAMS protected 'client' application and successfully completed the SAMS Partner Portal registration process, all required identity verification steps, and who has been authorized to access at least one (1) NVDRS SAMS-protected activity. - Users may be State government workers, contractors or interns. - Have full system permission including permission of the NVDRS state user plus exporting data, importing electronic records, and merging incidents for their assigned state.

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.	User Roles and permissions are used to minimize the amount of information exposed. All NVDRS Web users must first receive an invitation to join the Secure Access Management Services (SAMS) by the SAMS Activity Administrator (AA) via their business email address. The NVDRS CDC Administrator role also serves as the SAMS Activity Administrator (AA) and is the only user with the authority to invite users to obtain a user account. Users must request access to specific files needed to perform their job. The AA determines the application role to be assigned to each user, then assigns the appropriate permissions to that role. Users are required to login at least once annually (365 days) or they will lose access to their account and will have to reapply (invitation through ID proofing or reestablishment by AMS admin). All users are validated, authenticated, and authorized via the standard SAMS process. External State Users are authenticated via SAMS using username and password. Internal CDC Users and Administrator have PIV-enabled access to the system through SAMS by way of Active Directory.
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.	All users are required to take Privacy and IT Security Awareness training upon hire and annually thereafter. This training has been reviewed and is compatible with CDC requirements 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).	All users are required to complete annual training requirements that consist of Ethics and Compliance training, security awareness course and sign the acknowledgment of the CDC Rules of Behavior which has been reviewed and is compatible with CDC requirements.
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).	Records are retained and disposed of in accordance with the CDC Records Control Schedule (N1-442-09-1) and in accordance with contractual agreement. Record copy of study reports are maintained in the agency from two to three years in accordance with retention schedules. Source documents are disposed of when they are no longer needed by program officials. Personal identifiers may be deleted from records when no longer needed in the study as determined by the system manager, and as provided in the signed consent form, as appropriate. 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.

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.	Administrative Administrative controls include a system security plan, contingency plan, regular back up of files and storage of backups off site, role-based security awareness training, least privilege access enforced through Active Directory groups, separate user and privileged accounts for administrators, policies and procedures in place for retention and destruction of PII, and a corporate incident response team and incident response plans. Technical Controls include identification and authentication using unique user IDs, passwords, and smart cards, use of firewalls and intrusion detection/prevention systems, virus scanning software on all computers, and a security information and event management (SIEM) solution. Physical Controls include guards, identification badges, key cards, and closed-circuit TV.

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	**Privacy Analyst Review Date:**	5/15/2023
Privacy Analyst Comments:		**Privacy Analyst Days Open:**	

SOP Review

SOP Review Status:	Approved	**SOP Signature:**	JWO Signature.docx
SOP Comments:		**SOP Review Date:**	6/16/2023
		SOP Days Open:	38

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	7/19/2023
Agency Privacy Analyst Review Comments:	Reviewer: Jim Laskowski This PIA was originally reviewed and approved outside, I have attached the approved PIA in Supporting Document(s). This PIA is ready for SAOP review and approval.	**Agency Privacy Analyst Days Open:**	33

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	
SAOP Comments:	Approved outside Archer on 6/23/2023	**SAOP Review Date:**	7/28/2023
		SAOP Days Open:	9

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
OMB Collection_NOA 2021.pdf	85199	.pdf	5/5/2023 12:18 PM	0
Response to PIA Comments_05May23.docx	18931	.docx	5/5/2023 12:26 PM	2

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 2	BANKS, Quentin	5/5/2023	The last approved PIA had Business Partners/Contacts & Vendors/Suppliers/Contractors selected as well. Why were they not selected? If this tool is no longer collecting PII from them, please explain why not. When did you stop? Who authorized it? Is their data still within this tool? If so, why? If not, when was the data removed? How was the data removed? Was the data destroyed? If so, how was it destroyed? If not, where is the data now? How is the data being secured? Who is protecting the data?	
PIA - 9	BANKS, Quentin	5/5/2023	Patients are members of the public; therefore you should select that as well.	
PIA - 10B	BANKS, Quentin	5/5/2023	This date expires in 2 months. Please confirm if a new date has been posted.	
PIA - 16	BANKS, Quentin	5/5/2023	Please define the acronyms on their first use: BSI	
PIA - 19	BANKS, Quentin	5/5/2023	What is the system administrator`s process to determine who has access to the PII? What`s the reason for those individuals to have the access?	
PIA - 2	COLLINS, LaQuawn PATEL, Anusha	5/9/2023	Business Partners/Contact & Vendors/Suppliers/Contractors were previously selected on the last PIA incorrectly because this information is collected and stored in SAMS. NVDRS Web does not collect this information, but this information remains in SAMS. How do I address this on the PIA?	