Save

Privacy Impact Assessment Form

v 1.47.4

Status: Draft | Form Number: F-34770 | Form Date: 2/13/2019 9:00:24 AM

	Question	Answer
1	OPDIV:	CDC
2	PIA Unique Identifier:	P-9871509-939253
2a	Name:	National Violent Death Reporting System Web Enablement (NVDRS Web)
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: Deputy Branch Chief POC Name: Leroy Frazier POC Organization: NCIPC/DVP/Surveillance Branch POC Email: lif6@cdc.gov POC Phone: 770.488.1507
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	May 10, 2019 □ Not Applicable

Save

11	Describe the purpose of the system.	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.
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 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 will be based on a centralized, web-based architecture, where a centralized database is hosted and maintained at the Center for Disease Control and Prevention (CDC) and accessed by funded states and their contracted partners (e.g., vital statistics, coroner/medical examiners, law enforcement) via an Internet browser. Information on deaths are 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. Each state's own Violent Death Reporting System establishes the details of that state's cases from primary and secondary data sources. Primary data sources are: Death Certificates (DC), Coroner/Medical Examiner (CME) reports, Law Enforcement Reports (LE). Secondary or optional data sources are: Child Fatality Review (CFR) data, Intimate Partner Violence (IPV) data, Toxicology Reports and Hospital Discharge ICD9/10 Codes data. Patients' complete medical records are not available in this system. Every record within NVDRS Web has an associated unique identifier. The combination of the following three field values make up a record identified to allow a match to an incident such as the Incident year, incident state, and incident number. The combination of two or more of the following field values make a probabilistic or an exact match to an incident such as the 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 birth day of month (1-31), last four digits of victim's coroner/medical examiner record number, last four digits of victim's death certificate record number, and abstractor-assigned manner of death. Social Security Numbers (SSN), in full or in part, are not captured. Users authenticate via Secure Access Management Services (SAMS) and Active Directory (AD) using their email addresses as their userid and a password. This information is stored permanently or until contract ends.

13	Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.	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. 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. NVDRS collects facts from four major sources about the same incident, and pools information into a usable, anonymous database. An incident can include one victim or multiple victims. The four major data sources are death certificates, coroner/medical examiner reports, law enforcement reports, and crime laboratories. The facts collected are about violent deaths which includes circumstances related to suicide such as depression and major life stresses like relationship or financial problems, relationship between the perpetrator and the victim – for example, if they know each other, other crimes, such as robbery, committed along with homicide, and multiple homicides, or homicide followed by suicide. As data become available through the NVDRS on line database, state and local violence prevention practitioners use it to guide prevention programs, policies, and practices by identifying common circumstances associated with violent deaths of a specific type (e.g., committed during a crime such as robbery, gang violence, or intimate partner violence) or a specific area (e.g., a cluster of suicides); assisting groups in selecting and targeting violence prevention efforts; supporting evaluations of violence prevention activities; and improving the public's access to in-depth information on violent deaths. Complete medical records are not available in this system. SAMS and AD are the authentication mechanism for access to NVDRS Web Application hosted in the CSAMS environment and both have their own PIA. Access is extended via invitation only. Non-identifiable demographic, circumstance, and narrative (case description) data related to violent deaths is collected. This information is stored permanently or until contract ends.
14	Does the system collect, maintain, use or share **PII**?	● Yes ○ No

Save

15	Indicate the type of PII that the system will collect or maintain.	□ Social Security Number □ Name □ Driver's License Number □ Mother's Maiden Name ☒ E-Mail Address □ Phone Numbers □ Medical Notes □ Certificates □ Education Records □ Military Status □ Foreign Activities □ Taxpayer ID Sex Age zip code birth day of the month □ Date of Birth □ Photographic Identifiers □ Biometric Identifiers □ Vehicle Identifiers □ Mailing Address □ Medical Records Number □ Financial Account Info □ Legal Documents □ Device Identifiers □ Employment Status □ Passport Number
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?	500-4,999
18	For what primary purpose is the PII used?	For identity Proofing on SAMS, contact and follow-up.
19	Describe the secondary uses for which the PII will be used (e.g. testing, training or research)	None
20	Describe the function of the SSN.	N/A
20a	Cite the **legal authority** to use the SSN.	N/A
21	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).
22	Are records on the system retrieved by one or more PII data elements?	○ Yes ● No

Save

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.	OMB Approval Number 0920-1240 Expiration Date 08/31/2021
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.	There is no process in place because the only item being collected are email addresses.
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.	If the external organization/individual want access to NVDRSWeb, then there is no method for individuals to opt-out of the collection of PII because the only item being collected are email addresses.
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.	An application is set up to use SAMS by external partners who would like access to NVDRSWeb. An email notification is sent to external partners and then they are granted access to the application. Once external partners invitations have expired, they must reapply via the Informatics Service Desk to get assistance to access the system.
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.	To resolve an individual's concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate, individuals should contact the Management Information Systems Office (MISO), Informatics Service Desk at 1-855-644-8244.

Save

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.	System and Security Stewards review PII contained in the system annually (every 365 days), concurrent with resubmission of the system PIA and review of the BSI. Integrity and availability are checked by the system steward on an ongoing basis, in the course of initiating and terminating user accounts. Relevancy of the PII in the system (which is limited to names and email addresses of the system users) is defines user groups and access levels. NVDRS undergoes at least one enhancement effort each 365 days, during which the availability and relevancy of the entire data dictionary are assessed and updated according to program needs.	
31	Identify who will have access to the PII in the system and the reason why they require access.	☐ Users	
		☒ Administrators	The administrator need access to identity proof on-boarding users NVDRS via SAMs.
		☐ Developers	
		☐ Contractors	
		☐ Others	
32	Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	The CDC uses the concept of role-based access control (RBAC) to give the appropriate permissions associated with each user role. RBAC uses the security principle of least privilege which	
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.	The least privilege model will be used to allow those with access to PII to be able to access the minimum amount of PII needed to perform their job. Users must request access to specific files needed and that is the only access they are permitted. No one will be granted more access than is necessary to perform their job.	
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.	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.	
35	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.	
36	Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?	● Yes ○ No	

Save

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 (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 for computer 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.
38	Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.	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.
39	Identify the publicly-available URL:	http://www.cdc.gov/violenceprevention/nvdrs/
40	Does the website have a posted privacy notice?	● Yes ○ No
40a	Is the privacy policy available in a machine-readable format?	● Yes ○ No
41	Does the website use web measurement and customization technology?	● Yes ○ No

Save

		Technologies	Collects PII?
41a	Select the type of website measurement and customization technologies is in use and if it is used to collect PII. (Select all that apply)	☐ Web beacons	○ Yes ○ No
		☐ Web bugs	○ Yes ○ No
		☒ Session Cookies	○ Yes ● No
		☐ Persistent Cookies	○ Yes ○ No
		Other...	○ Yes ○ No
42	Does the website have any information or pages directed at children under the age of thirteen?	● Yes ○ No	
42a	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?	○ Yes ● No	
43	Does the website contain links to non- federal government websites external to HHS?	● Yes ○ No	
43a	Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?	○ Yes ● No	

General Comments	Q40a: In accordance with HHS's "Rescission of Office of the Chief Information Officer/Superseded Policy for Machine Readable Privacy Policies and Related Guidance Documents" memo. MRPP cannot be validated due to obsolete technology and the suspension of work on P3P by the Platform for Privacy Preferences Project workgroup.
OPDIV Senior Official for Privacy Signature	Jarell Oshodi -S Digitally signed by Jarell Oshodi -S Date: 2019.04.15 11:00:53 -04'00'