Save

# Privacy Impact Assessment Form

v 1.47.4

Status: Draft | Form Number: F-27829 | Form Date: 9/20/2016 9:28:38 AM

| | Question | Answer |
|---|---|---|
| 1 | OPDIV: | CDC |
| 2 | PIA Unique Identifier: | P-6028314-852030 |
| 2a | Name: | School Associated Violent Deaths Surveillance System (SAVD-SS) |
| 3 | The subject of this PIA is which of the following? | ○ General Support System (GSS)<br>○ Major Application<br>○ Minor Application (stand-alone)<br>◉ Minor Application (child)<br>○ Electronic Information Collection<br>○ Unknown |
| 3a | Identify the Enterprise Performance Lifecycle Phase of the system. | Implementation |
| 3b | Is this a FISMA-Reportable system? | ○ Yes<br>◉ No |
| 4 | Does the system include a Website or online application available to and for the use of the general public? | ○ Yes<br>◉ No |
| 5 | Identify the operator. | ◉ Agency<br>○ Contractor |
| 6 | Point of Contact (POC): | POC Title: Business Steward<br>POC Name: Leroy Frazier<br>POC Organization: CDC/ONDIEH/NCIPC<br>POC Email: lif6@cdc.gov<br>POC Phone: 770.488.1507 |
| 7 | Is this a new or existing system? | ◉ New<br>○ Existing |
| 8 | Does the system have Security Authorization (SA)? | ○ Yes<br>◉ No |
| 8b | Planned Date of Security Authorization | October 7, 2016<br>☐ Not Applicable |

Save

| | | |
|---|---|---|
| 11 | Describe the purpose of the system. | A school-associated violent death is defined as a homicide, suicide, or legal intervention in which the fatal injury occurred 1) on the campus of a functioning public or private elementary or secondary school in the United States, 2) while the victim was on the way to or from regular sessions at such a school, or 3) while the victim was attending or traveling to or from an official school-sponsored event. Cases will include deaths of students as well as non-students (e.g., faculty, school staff, family members, or community residents).<br><br>The School Associated Violent Deaths Surveillance System (SAVD-SS) will draw cases from the entire United States in an attempt to capture all cases of school-associated violent deaths that have occurred. SAVD-SS uses the collected data to describe the epidemiology of school-associated violent deaths, identify common features of these deaths, estimate the frequency and rate of school-associated violent deaths in the United States, and identify potential risk factors for these deaths. |
| 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.) | SAVD-SS will collect victim names, date of death, date of birth, manner and cause of death, location of death, circumstances surrounding the death (e.g., mental health problems, crises experienced by the victim). |

Save

| | | |
|---|---|---|
| 13 | Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily. | A school-associated violent death is defined as a homicide, suicide, or legal intervention in which the fatal injury occurred 1) on the campus of a functioning public or private elementary or secondary school in the United States, 2) while the victim was on the way to or from regular sessions at such a school, or 3) while the victim was attending or traveling to or from an official school-sponsored event. Cases will include deaths of students as well as non-students (e.g., faculty, school staff, family members, or community residents).<br><br>SAVD-SS will draw cases from the entire United States in an attempt to capture all cases of school-associated violent deaths that have occurred. Cases will be identified by CDC staff through a systematic search of computerized newspaper and broadcast media databases (e.g., Lexis-Nexis). To confirm the facts of each event, a brief interview will then be conducted with at least one law-enforcement officer familiar with the event (i.e., a police officer, police chief, or district attorney). For each confirmed case additional data will be obtained from three official sources: 1) law enforcement investigative reports; 2) structured telephone interviews with investigating law enforcement officials; and 3) structured telephone interviews with school officials (i.e., school principal, superintendent, school counselor, school teacher, or school support staff) who are familiar with the case in question. These sources will provide detailed information regarding victims, alleged offenders, the school associated with each death, and the circumstances of the fatal injuries.<br><br>SAVD-SS uses the collected data to describe the epidemiology of school-associated violent deaths, identify common features of these deaths, estimate the frequency and rate of school-associated violent deaths in the United States, and identify the potential risk factors for these deaths. The type of information collected are the victim names, date of death, date of birth, manner and cause of death, location of death, circumstances surrounding the death (e.g., mental health problems, crises experienced by the victim). |
| 14 | Does the system collect, maintain, use or share **PII**? | (•) Yes<br>( ) No |

Save

| | | |
|---|---|---|
| 15 | Indicate the type of PII that the system will collect or maintain. | ☐ Social Security Number<br>☒ Name<br>☐ Driver's License Number<br>☐ Mother's Maiden Name<br>☐ E-Mail Address<br>☐ Phone Numbers<br>☐ Medical Notes<br>☐ Certificates<br>☐ Education Records<br>☐ Military Status<br>☐ Foreign Activities<br>☐ Taxpayer ID<br>☒ Date of Birth<br>☐ Photographic Identifiers<br>☐ Biometric Identifiers<br>☐ Vehicle Identifiers<br>☐ Mailing Address<br>☐ Medical Records Number<br>☐ Financial Account Info<br>☒ Legal Documents<br>☐ Device Identifiers<br>☐ Employment Status<br>☐ Passport Number |
| 16 | Indicate the categories of individuals about whom PII is collected, maintained or shared. | ☐ Employees<br>☒ Public Citizens<br>☐ Business Partners/Contacts (Federal, state, local agencies)<br>☐ Vendors/Suppliers/Contractors<br>☐ Patients<br>Other: Deceased public citizens |
| 17 | How many individuals' PII is in the system? | 500-4,999 |
| 18 | For what primary purpose is the PII used? | The primary purpose for which PII is used is confirmation of facts related to cases. |
| 19 | Describe the secondary uses for which the PII will be used (e.g. testing, training or research) | The secondary uses for which PII will be used are: (1) to describe the epidemiology of school-associated violent deaths; (2) to identify common features of these deaths; (3) to estimate the frequency and rate of school-associated violent death in the United States; and (4) to identify potential risk factors for these deaths. |
| 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) |

Save

| | | |
|---|---|---|
| 22 | Are records on the system retrieved by one or more PII data elements? | ○ Yes<br>◉ No |
| 23 | Identify the sources of PII in the system. | Directly from an individual about whom the information pertains<br>☐ In-Person<br>☐ Hard Copy: Mail/Fax<br>☐ Email<br>☐ Online<br>☐ Other<br>Government Sources<br>☐ Within the OPDIV<br>☐ Other HHS OPDIV<br>☒ State/Local/Tribal<br>☐ Foreign<br>☐ Other Federal Entities<br>☐ Other<br>Non-Government Sources<br>☐ Members of the Public<br>☐ Commercial Data Broker<br>☒ Public Media/Internet<br>☐ Private Sector<br>☒ Other |
| 23a | Identify the OMB information collection approval number and expiration date. | 0920-0604 Exp: 05-31-2019 |
| 24 | Is the PII shared with other organizations? | ○ Yes<br>◉ 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 to notify individuals that their personal information will be collected because they are deceased. |
| 26 | Is the submission of PII by individuals voluntary or mandatory? | ◉ Voluntary<br>○ 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. | There is no method to Opt-out of the collection of PII because individuals are deceased. |
| 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. | There is no process in place to notify and obtain consent from individuals whose PII is in the system because individuals are deceased. |
| 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. | Only PII on deceased individuals is collected. |

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. | The Database administrator and technical steward will periodically review the PII contained in the system against the spreadsheets/database from which the data is extracted to ensure the data's integrity, availability, accuracy and relevancy. | |
| 31 | Identify who will have access to the PII in the system and the reason why they require access. | ☒ Users | Initially necessary for case finding and case confirmation tasks |
| | | ☒ Administrators | Necessary for tasks associated with all core study data collection management processes |
| | | ☐ Developers | |
| | | ☐ Contractors | |
| | | ☐ Others | |
| 32 | Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII. | Role Based Access Control (RBAC) is used to determine who has access to PII. | |
| 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 is used to allow those with access to PII to be able to access the minimum amount of PII needed 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 provided mandatory security and privacy awareness training annually. | |
| 35 | Describe training system users receive (above and beyond general security and privacy awareness training). | Users are also provided a separate HIPAA specific training.<br><br>Policies and rules regarding the treatment and handling of such information are reviewed annually and education regarding them is provided as needed (e.g., when new staff are added to the study or new rules regarding sensitive implementation are implemented by CDC or HHS). This training instills awareness regarding such policies, the penalties for noncompliance, and the nature of the administrative, technical, and physical safeguards that have been implemented to insure the security and confidentiality of the study's records, and to protect against any potential threats or hazards to their security or integrity. During these trainings, staff are also required to sign security pledges and non-disclosure agreements acknowledging their agreement to uphold the aforementioned responsibilities and to adhere to the study's guiding policies and guidelines for data collection and management. | |
| 36 | Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices? | ◉ Yes<br>○ 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. As such, record copies 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 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.<br><br>Over the course of the study, the data will be reported in the aggregate, such that no individual case can be identified from the reports. Once data collection is deemed complete, all records bearing identities of the victim, alleged offenders, informants, schools and communities will be destroyed. |
| 38 | Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls. | During the study, data will be secured through the use of technical, physical, and administrative controls. Hard copies of data (i.e., law enforcement investigative reports and interviews with school and law enforcement personnel) will be kept under lock and key in the Division of Violence Prevention (DVP) secured offices. These offices are located in a secured facility that can be accessed only by presenting the appropriate credentials (i.e., guards, identification badges, Key cards, and smart cards). The building housing the Division of Violence Prevention (DVP) offices can only be accessed using a key card that has been previously authorized by CDC security.<br><br>Digital data will be stored and backed up nightly on-site. Data is secured using technical controls (i.e., two-factor user identification and authentication, passwords, vulnerability scanning, and firewalls ) that only allow access by authorized individuals. The access list is audited annually and as needed (e.g., when a staff member leaves the study). |
| General Comments | | |
| OPDIV Senior Official for Privacy Signature | Beverly E. Walker -S<br>Digitally signed by Beverly E. Walker -S<br>DN: c=US, o=U.S. Government, ou=HHS, ou=CDC, ou=People, 0.9.2342.19200300.100.1.1=1001440343, cn=Beverly E. Walker -S<br>Date: 2016.11.08 13:44:47 -05'00' | |