North Carolina Department of Health and Human Services
Division of Public Health (DPH)
NC-Violent Death Reporting System
Data Request Form

This form should be completed by researchers who are interested in accessing data from the North Carolina Violent Death Reporting System (NC-VDRS). The information provided in this form will be used to populate a Data Use Agreement (DUA) for NC-VDRS data. Once this form is submitted, NC-VDRS staff will review your request. NC-VDRS staff may reach out to you to ask clarifying questions, to discuss whether NC-VDRS data will be useful in answering your research questions, and to suggest alternative or additional data sources that may be useful for your research project. Reviewing and drafting agreements for complex data requests and projects involving researchers at multiple institutions may require additional time.

Submit this form, along with required supporting documentation (e.g., IRB materials) to Scott Proescholdbell, NC-VDRS Director, NC DPH Injury and Violence Prevention Branch, by email at scott.proescholdbell@dhhs.nc.gov or beinjuryfreenc@dhhs.nc.gov.

Information about Researcher Requesting Data ("Recipient")

Full Name: _____

Title: _____

Institution: _____

Phone: _____ Email: _____

Name and title of the authorized signatory official who will sign the DUA:

_____
Name

_____
Title

Note: many universities, colleges, and other research institutions do not permit their faculty, staff, and students to sign contracts, and instead have a designated signatory official who signs agreements on behalf of the institution with which the faculty, staff, or student is affiliated. Please consult your institution's policy and identify the authorized signatory official.

Use Case for the Requested Data

1. Will the Recipient be using the requested data for research?

- ☐ Yes- the data will be used for research (includes research that is determined by an Institutional Review Board to be exempt)
- ☐ No- the data will be used for non-research activities only (e.g., public health surveillance or public health practice)

2. If the Recipient will be using the requested data for research, has the Recipient's study been reviewed by an IRB?

☐ Yes- an IRB reviewed the study **(please submit a copy of the IRB application and IRB determination letter)**
☐ No - an IRB has not reviewed the study

3. Which of the following types of data is the Recipient requesting? Please see Appendix A: DPH Data Use Agreement Guide for definitions of the terms listed below.

☐ Deidentified data set
☐ Limited data set
Note: a data set is limited if it includes county, zip code, dates, etc. Please see Appendix A for more information.
☐ Identified data set
Note: a data set may be identified if it includes street address, etc. Please see Appendix A for more information.

Description of the Requested Data

1. Please describe the time period for the requested data (e.g., all data collected between 1/1/2013 and 1/1/2017):

_____

2. How often does the Recipient want to receive the data?
Note: the frequency with which DPH will provide the requested data set will be determined based on DPH program staff capacity and the availability of resources.

☐ This will be a one-time provision of data ☐ Annually

☐ Other _____

3. Has the Recipient consulted with DPH program staff about this data request prior to completing and submitting this Data Request Form?

☐ Yes ☐ No

4. The NC-VDRS team has developed a "General Use Data File," which contains information that in DPH's experience can be used to answer many different research questions and that omits certain data fields that have high rates of missingness. Is the Recipient requesting the General Use Data File or a tailored data set?

☐ General Use Data File ☐ Tailored data set

If Recipient is requesting a tailored data set, please list every data field that is being requested in the table below or, if requesting a high volume of fields, submit a list of fields as an attachment alongside this form. Please note that tailored data sets may have limitations that should be discussed with NC-VDRS staff and will be created based on DPH staff capacity and the availability of other resources.

Name of Data Field	Description/Notes
E.g., name	*First, last, middle initial*
E.g., specimen source	*Capillary/venous*

E.g., sex	*Male/female*

5. Will the requested data set be linked to other data sets? If yes, please briefly describe the other data set(s), how they will be linked, and how the final linked data set will be used:

6. Will the requested data set need to be accessed by any third-party vendors (e.g., a vendor that the Recipient contracts with to maintain the environment in which the data would be hosted)? If yes, please list the vendor's name and explain what agreements, if any, the Recipient has in place with the vendor to ensure the privacy and security of the data:

Agreement Information

1. What is the desired DUA effective date? _____

2. Is there a funding, publishing, or other deadline related to the desired effective date? If yes, please explain:

3. Please provide a brief description of how the data will be securely stored upon receipt:

4. Please provide a brief description of the project for which the data will be used:

5. What is the public health significance (if any) of this project?

_____

6. What will the results of the project be used for?

_____

7. Names of principal researcher and co-investigators, and others who will be permitted to access the requested data:

Name: _____ Role: _____

Name: _____ Role: _____

Name: _____ Role: _____

Name: _____ Role: _____

Name: _____ Role: _____

Name: _____ Role: _____

Name: _____ Role: _____

Name: _____ Role: _____

Name: _____ Role: _____

8. Are all of the individuals named above employed by the same institution? If no, please explain below. Additional DUAs may be needed for individuals employed at different institutions.

_____

9. Expected project completion date: _____

10. In which format would the Recipient prefer to receive the data?

☐ SAS
☐ CSV
☐ Other _____

Compliance with NC DHHS Privacy and Security Policies and Manuals

1. Please review the security requirements outlined in Appendix B of this Data Request Form. Is the Recipient able to comply with the requirements set forth in Appendix B?

☐ Yes- the Recipient is able to comply with the security requirements
☐ No- the Recipient is unable to comply with the security requirements

---

Submit this form, along with required supporting documentation (e.g., IRB materials) to Scott Proescholdbell, NC-VDRS Director, NC DPH Injury and Violence Prevention Branch, by email at scott.proescholdbell@dhhs.nc.gov

Appendix A: DPH Data Use Agreement Guide

Data set types: Deidentified v. Limited v. Identified

The following definitions of a deidentified, limited, and identified data set are included for the purpose of assisting the Recipient in accurately completing the Data Request Form and do not reflect actual data fields that may be collected and retained in NC-VDRS.

Deidentified data set

A data set is deidentified when it meets the standard set forth under 45 CFR §164.514(b). Specifically, a data set is deidentified when the following identifiers of the individual or the individual's relatives, employers, or household members are removed from the data set:

1. Names
2. All geographic subdivisions smaller than a state, including: street address, city, county, precinct, ZIP code, and their equivalent geocodes, except for the initial three digits of the ZIP code if, according to the current publicly available data from the Bureau of the Census:
    a. The geographic unit formed by combining all ZIP codes with the same three initial digits contains more than 20,000 people; and
    b. The initial three digits of a ZIP code for all such geographic units containing 20,000 or fewer people is changed to 000
3. All elements of dates (except year) for dates that are directly related to an individual, including birth date, admission date, discharge date, death date, and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older
4. Telephone numbers
5. Fax numbers
6. Email addresses
7. Social security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and series numbers, including license plate numbers
13. Device identifiers and serial numbers
14. Web Universal Resource Locators (URLs)
15. Internet Protocol (IP) address numbers
16. Biometric identifiers, including finger and voice prints
17. Full face photographic images and any comparable images
18. Any other unique identifying number, characteristic, or code

If a data set contains any of the 18 identifiers described above then the data set is not deidentified and may be considered a limited data set or an identified data set.

Limited data set

A limited data set ("LDS") is defined at 45 CFR §164.514(e) and excludes most, but not all, of the 18 identifiers that must be excluded in a deidentified data set.

A limited data set does not include the following information pertaining to an individual or the individual's relatives, employers, or household members:

1. Names
2. Street addresses
3. Telephone numbers
4. Fax numbers
5. Email addresses
6. Social security numbers
7. Medical record numbers
8. Health plan beneficiary numbers
9. Account numbers
10. Certificate and license numbers
11. Vehicle identifiers and serial numbers, including license plate numbers
12. Device identifiers and serial numbers
13. Web Universal Resource Locators (URLs)
14. Internet Protocol (IP) addresses
15. Biometric identifiers, including finger and voice prints
16. Full face photographic images and any comparable images

A limited data set does include the following information: some geographic information (such as town/city, state, and zip code- but not street addresses), dates (such as birth date, date of death, admission date, discharge date), and age (as described in years, months, days, or hours).

Identified data set

An identified data set is not defined under HIPAA, but is any data set that includes information beyond what is permitted to be included in either a limited data set or a deidentified data set. For example, any data set that includes names, telephone numbers, or street addresses would be considered an identified data set.

Questions?

If you have questions about the types of data sets described here or other questions about terms used in this Data Request Form, please contact Scott Proescholdbell, NC-VDRS Director, NC DPH Injury and Violence Prevention Branch.

Appendix B: Security Requirements

Compliance with Applicable Laws

The Recipient shall comply with all applicable laws, ordinances, codes, rules, regulations, licensing requirements, electronic storage standards concerning privacy, data protection, confidentiality, and security including those of federal, state, and local agencies having jurisdiction where business services are provided for accessing, receiving, or processing all confidential information.

State of North Carolina and Department of Health and Human Services Privacy and Security Requirements

The Recipient shall implement internal data security measures, firewalls, and other security methods utilizing appropriate hardware and software necessary to monitor, maintain, and ensure data integrity in accordance with all applicable federal regulations, state regulations, DHHS privacy and security polices, and local laws. The Recipient will maintain all security safeguards throughout the term of this DUA. In addition, the Recipient agrees to maintain compliance with the following:

NC DHHS Privacy Manual and Security Manual, both located online at:
https://policies.ncdhhs.gov/departmental/policies-manuals/section-viii-privacy-and-security

NC Statewide Information Security Manual, located online at: https://it.nc.gov/statewide-information-security-policies

Health Insurance Portability and Accountability Act (HIPAA)

If DPH determines that some or all the activities within the scope of this DUA are subject to the Health Insurance Portability and Accountability Act of 1996, P.L. 104-191, as amended (HIPAA), or its implementing regulations, the Recipient agrees to comply with all HIPAA requirements and will execute such agreements and practices as DPH may require ensuring compliance.

Confidentiality

Confidentiality: The Recipient shall protect the confidentiality of all information, data, instruments, documents, studies, or reports given to the Recipient under this DUA in accordance with the standards of the DHHS privacy and security policies, applicable local laws, state regulations, and federal regulations including: the Privacy Rule at 45 C.F.R. Parts 160 and 164, subparts A and E , Security Standards at 45 C.F.R. Parts 160, 162 and 164, subparts A and C ("the Security Rule"), and the applicable provisions of the Health Information Technology for Economic and Clinical Health Act (HITECH). The Recipient shall not disclose or make information available to any individual or organization without the prior written consent of DPH except as permitted by this DUA for performing its obligations. The Recipient acknowledges that in receiving, storing, and processing confidential information, it will implement necessary privacy and security measures to safeguard all information.

Encryption and Transmission: The Recipient will implement strong encryption algorithm that meets industry encryption standard criteria as defined by the National Institute of Standards and Technology (NIST) and HIPAA Security Standards to encrypt all confidential information including protected health information (PHI) and personally identifiable information (PII) while in transit to ensure data confidentiality and security.

Data Security: The Recipient shall implement internal data security measures, environmental safeguards, firewalls, access controls, and other security methods utilizing appropriate hardware and software necessary to monitor, maintain, and ensure data integrity in accordance with all applicable federal regulations, state regulations, local laws, and DHHS privacy and security policies. Data may not be shared further without written consent. In the event the Recipient obtains written consent by DHHS to enter into a third-party agreement to whom the Recipient provides confidential information, the Recipient shall ensure that such agreement contains provisions reflecting obligations of data confidentiality and data security as stringent as those set forth in the DUA.

Duty to Report: In addition to any DHHS Privacy and Security Office (PSO) notification requirement, the Recipient shall report all suspected and confirmed privacy/security incidents, including but not limited to privacy/security breaches involving unauthorized access, use, disclosure, modification, or data destruction to the DHHS Privacy and Security Office at ncdhhs.gov/about/administrative-divisions-offices/office-privacy-security within twenty-four (24) hours after the incident is first discovered. If the privacy or security incident involves Social Security Administration (SSA) data or Centers for Medicare and Medicaid Services (CMS) data, the Recipient shall report the incident within one (1) hour after the incident is first discovered. At a minimum, such privacy and security incident report will contain to the extent known: the nature of the incident, specific information about the data compromised, the date the privacy or security incident occurred, the date the Recipient was notified, and the identity of affected or potentially affected individual(s). During the performance of this DUA the Recipient is to notify the DHHS Privacy and Security Office of any contact by the federal Office for Civil Rights (OCR) received by the Recipient related to the Data under this DUA. In addition, the Recipient will reasonably cooperate with DPH to mitigate the damage or harm of such privacy/security incidents.

Cost Borne by Recipient: If any applicable federal regulations, state regulations, local law, or rules requires DPH or the Recipient to give affected individuals written notice of a privacy or security incident arising out of the Recipient's performance under this DUA the Recipient shall bear the cost of the notice.