

National Death Index (NDI) Supplemental Data Use Agreement

This Data Use Agreement is designed specifically for **EXTERNAL PARTIES**, which includes funding sources, sites, collaborators, contractors, or consultants. This agreement serves to ensure proper handling and use of data by all entities outside applicants' organization.

Name and title of the responsible party:

Organization name and mailing address:

Phone Number:

E-mail :

1. Will this organization (or individual) receive any of the identifying or identifiable death record information obtained from the NDI, state death records, and/or death record follow-back investigations?

Definition of "IDENTIFYING or IDENTIFIABLE death record information"—Any information on death certificates, other paper documents, or in computer files that by itself, or if linked with other records, would permit the identification of one or more individuals or establishments; for example, name(s), Social Security number, exact dates, addresses, and death certificate number. Even with the removal of direct identifiers and linkable study subject identification numbers, there is still a special concern that some combinations of the remaining variables could potentially be used to identify an individual. For example, a combination of date of birth, date of death, and/or cause of death is considered identifiable.

☐

Yes

☐

No

☐

Maybe

2. Does this organization (or individual) have any contractual or other rights to the identifying information referred to above?

☐

Yes

☐

No

☐

Maybe



If the answers to questions 1 and 2 are "No," then responding to questions 3 and 4, and signature of data steward and IT Manager or IT Director—are not necessary.

NDI Supplemental Data Use Agreement

3. In the box below, describe the following controls that would be used to store and maintain the confidentiality of the **IDENTIFYING or IDENTIFIABLE** death record information at your organization:

- **Physical controls**—building guards, identification badges, key cards, closed circuit TV, and locked offices.
- **Technical controls**—user identification, passwords, firewalls, encryption, virtual private network, intrusion detection system. All non-federal applicants must store and access the NDI data on a secure server of the affiliated institution or organization. The NDI data cannot be directly accessible from the Internet. Only federal agencies are permitted to store and access the NDI data on FedRAMP moderately approved cloud-based systems. The NDI data must stay behind the affiliated institutional or organization firewalls and must not be stored on portable devices or personal computers. Please be aware that the standard encryption requirement for sensitive federal information, like the NDI data, is FIPS-140-2 in accordance with NIST 800-53. NIST 800-53 is only intended for federal agencies. The parallel standard for non-federal entities is NIST 800-171.
- **Administrative controls**—frequency of backing up files, where backup files will be stored, methods to ensure least privilege access, methods for ensuring IDENTIFYING or IDENTIFIABLE death record information is not co-mingled with administrative records not part of this project, how use will be monitored to prevent use for purposes not approved for this project, how personnel using the system will be trained and made aware of their responsibilities for protecting the IDENTIFYING or IDENTIFIABLE death record information and methods for monitoring who has access to the data. Please include text indicating the number of persons who will have access to the backup files containing IDENTIFYING OR IDENTIFIABLE death record information.

***NOTE: If multiple sites are involved in the above-mentioned study project, each site must describe its own controls that would be used to maintain the confidentiality of the IDENTIFYING or IDENTIFIABLE death record information.

4. When and how will your organization destroy ALL electronic NDI identifiable data (including the data derivatives) received from the NDI? If you do not have a specific destruction plan, please explain.

****Note:** In accordance with NIST SP 800-88 Rev. 2, NCHS advises that, at a minimum, the Clear Sanitization Method should be applied when destroying electronic NDI identifiable data (including the data derivatives) received from the NDI.

For your reference, you can find further details on Guidelines for Media Sanitization on the CSRC website: [SP 800-88 Rev. 2, Guidelines for Media Sanitization | CSRC](#).

NDI Supplemental Data Use Agreement



Study or Project Title:

The undersigned hereby agrees to the following terms and conditions associated with this National Death Index (NDI) Application and to the use of the information obtained from NCHS National Death Index:

- A. Except for individuals or organizations specified in the approved NDI application, no data will be published or released in identifiable form to any party. **ALL REQUESTS FOR IDENTIFIABLE DATA OBTAINED VIA THE NDI WILL BE REFERRED IMMEDIATELY TO NDI STAFF.** In accordance with Section 308(d) of the Public Health Service Act, such identifiable data will specifically not be provided in response to a direct order from an official of any government agency, the Administration, or Congress, nor in response to an order from a court of justice.
- B. NDI data may only be used for public health and medical studies, PROVIDED that no actions are taken which may directly affect individuals or establishments.
- C. NDI data may not be used for genealogical, legal, administrative or commercial purposes and/or to generate profit. Furthermore, the NDI data may not be used for training any artificial intelligence algorithms.
- D. The identifying information will be used only for the study or project proposed and the purpose described in the approved NDI Application. Use of the information for a research project other than the one described in the application form will not be undertaken until after a separate NDI Application for that project has been submitted to and approved by the NDI.
- E. The National Center for Health Statistics (NCHS) obtains death record information via contracts with the state vital statistics offices. These contracts contain specific restrictions on the use of the information by the NDI and by the NDI Plus service (provides NDI users cause-of-death codes). By signing below, I understand that I am also providing the same assurances to the State Vital Statistics Offices. Violation of the terms and conditions of this Agreement may subject the organization/researcher to immediate abrogation of the Agreement by NCHS, the required return of all NDI data and related materials, and denial of future use of the NDI. Violation of the terms of the Agreement may also be a violation of federal criminal law under 18 U.S.C. § 1001. In the event of unauthorized disclosure of identifiable information from NDI data, NCHS will pursue all legal remedies. Violations of the terms of the Agreement are also subject to state legal remedies.
- F. The original version of the NDI data must be retained at a single location, and no copy or extract of identifiable information may be made available to anyone except those individuals identified in the NDI Application and those who have signed the NDI Data Use Agreement.
- G. All non-federal applicants must store and access the NDI data on a secure server of the affiliated institution or organization. The NDI data cannot be directly accessible from the Internet. Only federal agencies are permitted to store and access NDI data on FedRAMP moderate approved cloud-based systems. The NDI data must stay behind the affiliated institutional or organization firewalls and must not be stored on portable devices or personal computers.
- H. When releasing statistical information, the recipient will make every effort to avoid inadvertent disclosure. Counts, rates, and percentages for sub-national geographic areas will be suppressed and not displayed in any manner if they are based on 1 to 9 observations in the numerator, denominator, or total, regardless of the number of years combined. This data suppression rule applies to all text, tables, and figures (including maps) contained in main and supplemental files. No data on an identifiable case should be derivable through subtraction or other calculations from the combination of tables in a given publication. Data should not permit disclosure when used in combination with other known data.
- I. All applicants, except for data stored in registries, or other approved long-term studies, must indicate the month and year ALL NDI identifiable data -including the data derivatives- received from the NDI will be destroyed and submit Data Destruction Form (Attachment A).
- J. The organization/researcher agrees to report any confirmed or suspected losses, including theft and unauthorized disclosure/access, of personally identifiable information (PII) from the NCHS data file(s) to the CDC Computer Security Incident Response Team's (CSIRT) 24x7 Emergency Number (1-866-655-2245) within 1 hour of discovery. After notifying CSIRT, the organization/researcher will notify the Director of the NCHS Division of Vital Statistics with the incident number issued by CDC CSIRT. The organization/researcher will not communicate PII details via email.

NDI Supplemental Data Use Agreement

- K.** Authorized NDI staff or agents may, upon request, be granted access to [redacted] facilities, where confidential NDI data are kept or used, for the purpose of inspecting the data security arrangements.
- L.** I understand that while state and territory (jurisdictions) vital statistics offices may receive copies of this application, they may require additional information and/or assurances before responding to separate requests for copies of death certificates or for death record information directly from such them. They may not be able to honor certain requests because of the proposed uses of the state data. Furthermore, once data from a particular state or territory is received, I understand that users of the data are subject to jurisdictional laws and regulations relating to disclosure of information on individuals or establishments.
- M.** I confirm that I have carefully reviewed the NDI application. All the statements included in this application, as well as any related confidentiality assurances are true, complete, and accurate to the best of my knowledge and belief. My signing below, I am indicating my clear agreement to comply with all the statutorily based requirements outlined. I also acknowledge that knowingly or willfully making a false statement in any matter within the jurisdiction of any department or agency of the Federal government is a violation of 18 U.S.C. § 1001, and is punishable by a fine or imprisonment, or both.

**Note: Only recipients of identifiable NDI data are required to have this specific portion completed and signed.
The Data Steward is required to sign before the IT manager or IT Director.**

SIGNATURE of the Data Steward:

[redacted] [redacted]
Signature Date
[redacted]
Name (type or print)
[redacted]
Title
[redacted]
Organization
[redacted]
E-mail

SIGNATURE of IT Manager or IT Director:

[redacted] [redacted]
Signature Date
[redacted]
Name (type or print)
[redacted]
Title
[redacted]
Organization
[redacted]
E-mail

SIGNATURE of Principal Investigator, Project Director or Project Officer:

[redacted] [redacted]
Signature Date
[redacted]
Name (type or print)
[redacted]
Title
[redacted]
Organization
[redacted]
E-mail

***SIGNATURE of Official authorized to execute agreements (last person to sign and date):**

[redacted] [redacted]
Signature Date
[redacted]
Name (type or print)
[redacted]
Title
[redacted]
Organization
[redacted]
E-mail

*****NOTE:**

The "official authorized to execute agreements" is the person authorized to sign grant proposals, a company vice president, or a government division or bureau director. By signing this agreement as the authorized official, you are declaring that you have the authority to make the above assurances on behalf of the university, company, agency, or other organization and to bind the organization to the terms of this agreement and you take responsibility for the confidentiality assurances of your organizations or individuals who are participating in this study.