

# Application for Restricted Data

## INSTRUCTIONS:

Please provide the following information. Rename this PDF with your Last name, First initial, the short name of the Restricted Dataset (i.e. RPG-1, NCANDS, or Flint) and the word "Application". Example: "Doe, J. RPG-1 Application.pdf". Email it to NDACAN@cornell.edu.

**Application Date:** \_\_\_\_\_

**Restricted Dataset Number and Title:**

## I. Investigator

The Investigator serves as the primary point of contact for all communications involving the License. The Investigator must hold a faculty appointment or research position at the Investigator's Institution and assumes responsibility for compliance with all terms of the License by employees of the Investigator's Institution, including the day-to-day security of the Restricted Data electronic data files and printed output derived from the files.

**Investigator Name** \_\_\_\_\_

**Investigator Title** \_\_\_\_\_

**Investigator Institution** \_\_\_\_\_

**Investigator Department** \_\_\_\_\_

**Investigator Office Address** \_\_\_\_\_

**Investigator Email** \_\_\_\_\_

**Investigator Phone Number** \_\_\_\_\_

## II. Investigator's Use of the Restricted Data

1. For what purposes are you applying for the Restricted Data?

2. Describe all the ways the results of the research will be used, including plans for public dissemination:

3. All linking or merging of files must be pre-approved in writing by the Archive. Do you propose to link or merge the Restricted Data with other data files, including other years of the same series (e.g. NCANDS Child File)?

☐ Yes ☐ No

If Yes, provide the names and descriptions of these other files. Also, describe how the linking will be accomplished and explain why it is necessary to achieve your research objectives:

### III. Registration Status of the Investigator's Institution's Institutional Review Board

1. The Investigator's Institution must be an institution of higher education, research organization, or government agency that employs the Investigator. The institution must be registered with the U.S. Office for Human Research Protections. If the institution is not registered, the Archive may use the information in section III.2 to grant an exemption to institutions with a demonstrated record of using sensitive data according to commonly-accepted standards of research ethics.

**Does the Investigator's Institution have an Institutional Review Board that is registered with the U.S. Office for Human Research Protections (OHRP)?** ☐ Yes ☐ No

**If Yes, what is the IRB number listed at the [OHRP database for registered IRBs](#)?** IRB \_\_\_\_\_

2. If your Institution does not have an IRB assurance number, you must answer the following questions. Skip this section if you responded "Yes" to the previous question.

**Describe your Institution in detail. What kind of work does it do? Include the type of organization, its profit/non-profit status, and primary sources of revenue:**

**What experience does the Institution have in overseeing the use of sensitive research data by its staff? Please give specific examples:**

**Does your employer have policies regarding scientific integrity and misconduct, or human subjects research that cover the secondary analysis of survey data?** ☐ Yes ☐ No

Important: If Yes, submit a copy of these policies with your application.

### IV. Representative of the Investigator's Institution

The Restricted Data License (separate document) will be signed by an individual who has the authority to enter into legal agreements on behalf of the Investigator's Institution. Examples are President, Vice President, Dean, Provost, or Contracts Officer. Note that a Department Chair is not acceptable. Please provide the contact information of the Representative of the Investigator's Institution:

**Representative Name** \_\_\_\_\_  
**Representative Title** \_\_\_\_\_  
**Representative Department** \_\_\_\_\_  
**Representative Phone Number** \_\_\_\_\_  
**Representative Email** \_\_\_\_\_

### V. Research Staff

Research Staff are individuals, affiliated with the Investigator's Institution, other than the Investigator, who are authorized to access the data. Research Staff must understand the conditions of the License and sign and submit a Research Staff Form that will be approved by the Archive.

In the spaces below, provide the requested information for all individuals, besides the Investigator, who are authorized to access the Restricted Data. If additional space is required, provide the information on a separate page.

**Staff Person 1 Name** \_\_\_\_\_  
**Staff Person 1 Institution** \_\_\_\_\_  
**Staff Person 1 Title** \_\_\_\_\_

Staff Person 1 Email \_\_\_\_\_

Staff Person 2 Name \_\_\_\_\_

Staff Person 2 Institution \_\_\_\_\_

Staff Person 2 Title \_\_\_\_\_

Staff Person 2 Email \_\_\_\_\_

## VI. Data Security

To ensure the confidentiality of the individuals in the Restricted Data, the Archive requires that security provisions are taken to protect the data and any output derived from it. By signing the License, the Investigator and Research Staff agree to implement safeguards to prevent unauthorized access, by electronic or physical means, to the data and any output created from it. The Restricted Data may be copied to and stored on a network server, personal computer hard drive, or other device, provided that the data are protected by password or other secure measures to prevent unauthorized access.

All installations of the Restricted Data must have electronic security measures in place to prevent access to the confidential data from unauthorized individuals. In the table below, provide a comprehensive list of all devices on which the Restricted Data will be installed and indicate the electronic security measures that will be applied to each device. If additional space is required, continue the list on a separate page.

For devices that have access to the Internet, all four of the electronic security measures (i.e. Password Login, Restricted Directory Access, Virus Protection and Firewall Protection) must be in place for this License to be approved. For non-Internet devices, firewall protection is not required.

ID	Device Type: Indicate workstation, laptop, server, portable media, or other device	Internet Enabled? Check the box if the device has access to the Internet	Password Login: The device requires a login ID and password at startup and after a period of inactivity	Restricted Directory Access: The directories containing the data are restricted to authorized users who have logged in to the device	Virus Protection: Anti-virus software is installed on the device	Firewall Protection: Firewall technology is in place for devices that are connected to the Internet
1						
2						
3						
4						

In addition to electronic security measures, the devices on which the data have been copied must be physically secured to prevent theft of the device. In the table below, describe the physical security measures that are in place for each device. Examples of such protection include offices that are locked when unoccupied, storage in secure cabinets when the device is not in use, and monitored access to the building where the device is housed. If additional space is required, continue the list on a separate page. Be sure that the ID number of the device in this table corresponds to the ID number of the device in the previous table.

Applications that are deemed to have inadequate physical security measures in place will be denied.

ID	Location of the Device Indicate building name and office number where the device is located	Description of Physical Security: Describe the physical security of the device. Examples include offices that are locked when unoccupied, storage in secure cabinets when the device is not in use, and monitored access to the building where the device is housed
1		
2		
3		
4		

**Describe any other information relevant to the electronic or physical security of the Restricted Data:**

#### **NDACAN Review (Office Use Only)**

**Reviewer Comments**

**NDACAN Approval Date** \_\_\_\_\_