

*General Social Survey (GSS)*  
NORC

**OBTAINING GSS SENSITIVE DATA FILES**

The GSS geographic identification code files are made available to researchers under special contract with NORC. The GSS takes its promise of anonymity to its respondents very seriously and this is the basis for the contract process. Under contract, the GSS will provide data on State, Primary sampling unit, County, & Census tract, but in no circumstances will individually identifying information (name, address, etc.) be provided.

The procedure for obtaining the GSS Sensitive Data is outlined below:

- 1) Contact us to receive via e-mail “Obtaining GSS Sensitive Data Files,” which outlines the documentation and procedures required for approval.
- 2) After you return the documentation specified in “Obtaining GSS Sensitive Data Files” to us by e-mail, our review process for approval will start.
- 3) Once we approve your application, we will send you via e-mail the Contract/Order Form. You will return these to us along with a check for \$750.
- 4) We will send you a copy of the contract, a CD-ROM with the data requested, and documentation on the area variables. You must merge the data included on the CD-ROMs with your own GSS dataset.

The process can take several months. To avoid delays, we ask potential users of these Sensitive Data files to be prepared to submit the following for the review process for approval (more information is contained in “Obtaining GSS Sensitive Data Files”):

- 1) **Research Plan** – Include a specification of which area datasets & variables you intend to use. The Research Plan must fully specify all of the research that is to take place using the data and must be project specific.
- 2) **Curriculum Vitae** – One for each participating research staff
- 3) **Sensitive Data Protection Plan** - Study the “Criteria for Sensitive Data Protection Plans” and submit a Sensitive Data Protection Plan meeting all of its standards.
- 4) **Human Subjects Review Clearance** - Obtained from the appropriate body at your Institution, using the Sensitive Data Protection Plan as part of the application for approval.

To request further instructions, any of the documents mentioned above, or questions regarding the process in general, please contact the GSS at

GSS@NORC.org  
773-256-6288

Thank you for your interest in the GSS. We look forward to hearing from you.

## 2. OBTAINING GSS SENSITIVE DATA FILES

The GSS geographic identification code files are made available to researchers under special contract with NORC. The GSS, like most interview-based surveys, has promised anonymity to its respondents. This promise is taken very seriously and is the basis for the contract process. And, of course, no individually identifying information (name, address, and so on) will be provided, even under contract.

The process for obtaining the GSS Sensitive Data is outlined below. Institutional bureaucracies being what they are, the process can take several months, although it has been done in three weeks. In order to avoid needless delays, we recommend that potential users of these Sensitive Data files take the following steps, in the following order, **submitting all documentation at one time**:

1. **GSS Geographic Data Available** – These include state (1973 and later), primary sampling unit (1973+), county (1993+), and Census tract (2004+).
2. **For information about these files contact the GSS:** GSS@NORC.org or (773) 256-6288.
3. **Research Plan** – Submit a written Research Plan, and for the Geocode files, include a specification of which area variable you intend to use. The Research Plan must fully specify all of the research that is to take place using the data and must be project specific. It is not permitted, for example, for a faculty member to obtain the data for his/her own research project and then “lend” the data to a graduate student to do related dissertation research, unless this use is specifically stated in the research plan.
4. **Curriculum Vitae** -Submit a copy of your academic resume or *curriculum vitae* as well as all participating research staff to the address noted below.
5. **Sensitive Data Protection Plan** -Study the “Criteria for Sensitive Data Protection Plans” and investigate mechanisms that are available to you to meet its requirements at your site. Submit a Sensitive Data Protection Plan. The reviewers will examine the plan and may require some amendments. If the computing systems/environment change (e.g., move from a mainframe to a microcomputer-based system), a new Sensitive Data Protection Plan based on the new system must be submitted and approved. Laptop computers are not permitted for sensitive data research.
6. **Human Subjects Review Clearance** -Obtain Human Subjects Review Clearance from the appropriate body at the Receiving (your) Institution, using the Sensitive Data Protection Plan as part of the application for approval. Submit a copy of the approval/waiver to our office with all other required documentation.
7. **Contract for Use of Sensitive Data** -Upon approval of the Sensitive Data Protection Plan and application materials, a “Contract for Use of Sensitive Data” will be sent. Please note the following:

- a) There must be a Co-Investigator in situations in which the Investigator does not have a full-time permanent faculty-level appointment at the institution where the research will take place (e.g., where the Investigator is a visiting scholar or a graduate student). The Co-Investigator must be a PhD level, full-time faculty member at the Receiving Institution.
  - b) All original data files must be returned to GSS within the specified time limits (see Section III.L. of the Contract). All files and paper printouts containing GSS Sensitive Data or data derived from the GSS Sensitive Data must be destroyed or returned prior to the completion of the contract. A Certificate of Compliance, stating that all GSS Sensitive Data have been returned or destroyed, must be signed and returned before the contract is closed. Extensions to the timeframe stated in the contract will be addressed on an as needed basis.
  - c) There is a requirement that the Investigator(s), the Co-Investigator and the Receiving Institution assume liability, up to \$100,000, for any violations of the contract by any person at the Receiving Institution. If the institutional representative has issues with the liability language in the contract (Section III.L.), please contact the GSS representative immediately. The contract will not be approved without a liability section.
8. The Investigator will be sent an e-version of the sensitive data contract for signature.
- a) The Investigator(s), Co-Investigator (if any) and the Research Assistants, and Representative of the Receiving Institution must print out and sign three originals of the contract. The Representative is someone authorized to enter into contractual agreements on behalf of the Receiving Institution.
  - b) Send all three signed originals of the contract to the GSS representative.
  - c) After NORC representatives sign the contracts, a signed original will be returned to the Investigator, along with the data, unless otherwise noted. If the Receiving Institution requires more than one original, please make extra copies before the signature process begins and submit all of the original contracts together.
9. **Administrative Fee** – A check, made out to “NORC”, must be submitted along with the contracts. The \$750 non-refundable fee covers the expense of creating and shipping the data files and documentation, for up to four hours of consultation with the GSS staff, and the cost of administering the contract.

Note: If the Investigator changes institutions, the current contract is no longer valid and a new contract must be completed. Also, the original data and any analysis files must be returned to the GSS until the new contract is established. If the Investigator wishes to continue to use the data, a new Sensitive Data Protection Plan and Contract are required. A new fee must be submitted with the new contract before the original data will be returned.

All of the requested documentation should be mailed to the GSS:

**Jibum Kim**  
**NORC**  
**1155 E. 60<sup>th</sup> st.**  
**Chicago IL 60637**

If you have any questions regarding the **paperwork** process, please contact:

GSS  
GSS@NORC.org  
773-456-6288

Thank you for your interest in the GSS. We look forward to hearing from you.

## **2.1. CRITERIA FOR SENSITIVE DATA PROTECTION PLANS**

The “Contract for Use of Sensitive Data from the General Social Survey” (GSS) requires that potential investigators submit for approval by the GSS staff a Sensitive Data Protection Plan. This requirement is part of the effort to ensure that the promise of anonymity to the GSS respondents is kept and that no persons other than those authorized by the contract (the named Investigator(s), Co-Investigator, and Research Staff) have access to the contents of the Sensitive Data files.

### **Definitions**

In drafting the Sensitive Data Protection Plan, keep in mind the following definitions:

1. “Sensitive Data” includes any data from the GSS that might compromise the anonymity or privacy of respondents to those studies. Specifically, it includes any data file that, for either individuals, or families, includes:
  - a) Identification numbers or demographic information (such as month and year of birth, age, ethnicity, occupation, industry, gender, etc.);
  - b) geographic identification of areas smaller than Census Division, including, but not limited to state, county, minor civil division, primary sampling unit (PSU), segment, city, place, zipcode, tract, block numbering area, enumeration district, block group, or block;
  - c) any variables or fields derived from the data mentioned in items a)-b) above, including data linked to a GSS dataset using the data mentioned in items a) and b) above as linking or matching variables.
2. “Authorized Person” includes the named Investigator(s), Co-Investigator, and Research Staff. With the partial exception of some computing center personnel noted below, all other persons are referred to as “unauthorized person”.

## General Requirements:

GSS Sensitive Data must be stored either on CDs or removable storage devices that are kept in a locked storage location (i.e., in a locked desk, in a locked office) or within the password-protected hard-drive of a free-standing desktop PC on a directory that is *not networked*. The GSS Sensitive Data may not be analyzed within a directory that is networked. This requirement is mandatory, even in the case of additional protections such as firewalls and passwords. Please note that storing GSS Sensitive Data on laptop computers is not permitted.

The Sensitive Data Protection Plan must address each of these issues:

- 1 A description of the computing environment in which the named research staff will be managing and analyzing the data. For each item of computing equipment and removable storage devices to be used (tape drives, hard disks, CPU, disks, printers, flash drives, etc.), describe the following: a) their location; b) persons who have physical access to them; c) the security provisions that restrict access to use of data on the system(s), such as locked doors, locks on equipment, passwords, etc; d) the routine procedures for making backup copies of data files on any storage devices.
- 2 Include a description of how access to GSS Sensitive Data files located on the desktop computer will be limited to only authorized personnel. The description should include details of security measures, such as passwords and read/write access to the relevant files.
- 3 The plan must indicate how routine backups of the Sensitive Data will be prevented. The plan must include a statement that no more than one backup copy will be made of any file containing Sensitive Data and this copy will be destroyed (written over or otherwise made unreadable) prior to the return of the GSS Sensitive Data.
- 4 A description of how access to any removable storage devices such as CD ROM's, flash drives, diskettes, or tapes will be restricted. Include such information as where the CD ROM's/flash drives/diskettes/tapes are physically located and how physical access to them is to be restricted, including provisions for storage in locked cabinets when not in use. If you will not be using removable storage devices, clearly state this in your plan.
- 5 Include a description of how access to paper printouts containing Sensitive Data will be restricted. The GSS Sensitive Data Plan reviewers strongly recommend against the creation of any paper printouts containing Sensitive Data. If paper printouts must be used, the plan must clearly state why no other storage media could be used. Additionally, storage issues must be addressed, such as locked storage; how the printouts will be kept from the vision and reach of unauthorized persons when in use; and how the printouts will be destroyed (made unreadable). If printouts will not be used, simply state this in the plan.
- 6 Treatment of data derived from the sensitive data: We require a clear statement that you will treat all data derived from sensitive data in the same manner as the original sensitive data, and that you understand that data derived from sensitive data includes but is not limited to: a) subsets of cases or variables from the original sensitive data; b) numerical or other transformations of one or more variables from the original sensitive data, including sums, means, logarithms, or products of formulas; c) variables linked to another dataset using variables from a GSS sensitive dataset as linkage variables. (Aggregate statistical summaries of data and analyses such as tables and regression formulae are not "derived variables" in the sense used in this Agreement, and are not subject to the requirements of the Sensitive Data Protection Plan and Agreement).
- 7 Indicate which other GSS and non-GSS datasets, if any, you intend to link to the GSS sensitive data you are requesting, and include a clear statement that you will not perform linkages to any other datasets. Your statement must include recognition of the following rule that no GSS sensitive dataset may be linked to any other GSS sensitive dataset without the explicit written permission of GSS.