Attachment 10

CHIS Data Security Policies

10A: CHIS Data Collection Security Policies

10B: CHIS Data Access Center Policy and Procedures

10C: CHIS Data Delivery Protocol

California Health Interview Survey (CHIS)
Data Collection Security Policies

The data collection contractor for the California Health Interview Survey will have the primary responsibility to ensure the protection of any identifiable data on respondents. In its contract, the data collection contractor will be required to abide by the UCLA human subject research guidelines. Specific confidentiality protection procedures follow:

- **Secured Electronic Access to Raw Data:** All data will be stored electronically on computers with secured access. Only designated individuals will have access to the raw survey data.

- **Secured Backup of Data:** Backups of data files will be stored in a separate locked facility. Access to these files will be limited to designated individuals and only in case of emergency (e.g. primary data source destroyed by fire).

- **Consent for Contact Information:** After confirming or providing their address information near the end of the survey, the CHIS adult respondents are asked if they would be willing to participate in follow-up surveys. Respondents are provided with three choices: (1) Yes; (2) Maybe; and (3) Definitely No. If respondents answer “yes” or “maybe,” they are considered to have given contact consent to be re-contacted for follow-up studies. If the respondent refuses, then the interviewer will thank the respondent for participating in the survey and terminate the interview.

- **Separation of Contact Data from other Data:** At the completion of data collection, the data collection contractor will separate the contact data (name and address, if collected, as well as telephone numbers) and any other data items that may reveal the identity of the respondent (e.g. birthdate). This information will be stored in an ID file, which will be archived with secured access.

- **Data Deliverables without Respondent Identifiers:** The data collection contractor will deliver analysis data files without the ID file to the CHIS PI at the UCLA Center for Health Policy Research. Only month and year of birth will be included in the analysis files delivered to the Center.

- **Destruction of the ID File:** This information will be stored in two separate ID files: one that contains contact data on respondents who have agreed to be re-contacted for potential follow-back studies (ID_Recontact_OK) and another that contains information on all other CHIS respondents. The ID file for potential follow-back study participants (ID_Recontact_OK) will be archived by the data collection contractor for seven years effective at the completion of the data collection. Unless requested by the CHIS PI at UCLA for an extension, the ID file (ID_Recontact_OK) will be destroyed at the end of the five-year period. The ID file for CHIS respondents who have not agreed to be re-contacted for follow-back studies (ID_No_Recontact) will be maintained for 90 days after delivery of the final data file and then destroyed.

- **Data Access Center:** Storage of data received from the data collection contract and how data is released and disseminate is outline in the attached Data Access Center Policies and Procedures and the Data Delivery Protocol.

Policies and Procedures Governing Access to Confidential CHIS Data Through the Data Access Center

October 15, 2009

California Health Interview Survey (CHIS)
UCLA Center for Health Policy Research
10960 Wilshire Blvd., Suite 1550
Los Angeles, CA 90024
Fax: (310) 794-2684
Web: http://www.chis.ucla.edu
Email: chis@ucla.edu

Table of Contents

1. Background and Purpose

a. Background

The California Health Interview Survey (CHIS) is a population-based random-digit dial telephone survey of California residents conducted every two years since 2001. CHIS is the largest health survey conducted in any state and one of the largest health surveys in the nation. CHIS is conducted by the UCLA Center for Health Policy Research in collaboration with the California Department of Public Health, the California Department of Health Care Services, and the Public Health Institute. CHIS collects extensive information for all age groups on health status, health conditions, health-related behaviors, health insurance coverage, access to health care services, and other health related issues. Within each household, separate interviews are conducted with adults (age 18 and over), adolescents (ages 12-17), and parents of children (ages 0 to 11).

CHIS is designed to provide data that will support policy analysis, development, and advocacy, program planning and evaluation, and research. Given the public service nature of this research project, CHIS data are made widely available to a broad array of users while maintaining the confidentiality of CHIS respondents. CHIS data are made available through multiple channels, including publications, public-use data files, confidential data files, and through an Internet query system called *Ask*CHIS.

The Data Access Center (DAC), a secure data analysis facility operated by the UCLA Center for Health Policy Research (UCLA-CHPR), exists principally to support the preparation and maintenance of confidential CHIS data files and to conduct analysis of confidential CHIS data for research projects. Additionally the DAC supports the preparation and review of CHIS data files for dissemination, provides technical assistance to CHIS data users, and provides remote access analysis and programming services for external researchers with approved DAC projects.

Access to confidential CHIS data is available through the DAC. Analyses will be performed by CHIS and UCLA-CHPR statistical programming staff on behalf of qualified researchers who apply to the DAC for use of the confidential CHIS data in specific research studies and whose applications are approved by the CHIS Principal Investigator, following review and recommendation by the CHIS Data Disclosure Review Committee.

b. Purpose of this document

This document specifies the policies and procedures governing researcher access to the confidential CHIS data files maintained in the DAC. It describes the organizational structure of the DAC, the process by which investigators may apply for access to confidential CHIS data through the DAC, the methods by which researchers may be granted access to the data, and the physical, staff, and network security measures in place at the DAC. The policies and procedure for other CHIS-related functions of the DAC, such as confidential data file delivery, preparation of public-use data files, etc., are documented in the *CHIS Confidentiality Manual.*

c. General security information

The UCLA Center for Health Policy Research is responsible for leading and managing CHIS, obtaining the financial and other resources needed to conduct the survey, preparing, maintaining, and disseminating

CHIS data files, reporting the survey findings, and disseminating the survey results. The protection of the confidentiality of the CHIS respondents is an important and integral part of UCLA-CHPR's responsibilities.

All CHIS confidential data files are maintained at the DAC, which is designed to protect the confidentiality of CHIS respondents while facilitating analysis of confidential CHIS data for approved research studies in a secure, controlled environment. The DAC is located in the offices of the UCLA Center for Health Policy Research, 10960 Wilshire Blvd., Suite 1550, Los Angeles, CA 90024.

d. Staff confidentiality procedures

All UCLA-CHPR and CHIS staff whose duties require access to CHIS confidential data are given a copy of the *CHIS Confidentiality Manual* and this DAC policies and procedures document. They are also required to attend a one-hour internal training on confidentiality and policies and procedures to protect confidential data. All new CHIS staff members are required to have this training before accessing CHIS data. This training is repeated annually for all staff who may have need to access confidential CHIS data.

Upon completion of training, staff are required to sign a CHIS Affidavit of Nondisclosure. The statements are renewed annually. The original signed statements are filed with the Data Access and Confidentiality Manager, and a copy is provided to the employee.

e. Overview of DAC access & functions for research

The DAC is a secure, physical space within the UCLA-CHPR housed behind a locked, key-card accessible door providing restricted access only to authorized UCLA-CHPR employees.

Two groups of employees at the UCLA-CHPR have access to confidential CHIS data within the DAC:

1. Designated CHIS staff, and
2. Designated UCLA-CHPR Statistical Support & Programming (SSP) staff

No other UCLA-CHPR employees, data users, or other persons have physical access to confidential CHIS data files within the DAC.

Within the DAC, CHIS and SSP staff perform the following functions:

- Maintain confidential CHIS data files
- Coordinate DAC activities
- Prepare CHIS data files for analysis (cleaning, editing, coding, imputation, etc.)
- Prepare CHIS data files for delivery outside of the DAC
- Conduct analyses of CHIS data
- Conduct disclosure risk of CHIS data files and statistical output
- Provide technical assistance to CHIS data users
- Provide remote access analysis and programming services to external researchers with approved DAC projects

f. Confidential CHIS data: Identifiable and sensitive

CHIS data do not include direct identifiers — such as full name, telephone number, or social security number — that could be used to directly re-identify a survey respondent. Information collected through CHIS is self-reported by respondents, collected principally for research purposes, and does not include

information from health providers or medical records; it is not, therefore, subject to the Health Insurance Portability and Accountability Act (HIPAA) regulations.

Confidential data elements necessary for data collection, such as telephone number and exact birth date, are separated from other CHIS data by Westat, the subcontractor that conducts the CHIS interviews, and are never released from Westat, sent to UCLA, or made available in the DAC. The respondent's phone number is destroyed either 6 months after data collection or, if the respondent provides permission to participate in a follow-back study, 5 years after data collection.

CHIS collects detailed geographic information about the location of a respondent's residence that could lead to the deductive re-identification of a respondent. The most detailed geographic information in CHIS is **latitude/longitude** and **Census tract block group**. Due to the enhanced risk of deductive re-identification of survey respondents, these data elements are considered identifiable by the CHIS Principal Investigator. These variables are separated from the main CHIS data files and maintained in a separate access-restricted folder on the DAC's secure network. Other variables in the confidential data files include less detailed geographic information, such as zip code; even zip code can potentially increase the risk of re-identification when combined with detailed demographic characteristics. Some variables have verbatim responses that could potentially contain information that could be used to re-identify a respondent.

Finally, the confidential files at the DAC contain sensitive information, such as information about sexual behavior, mental health conditions, violence, alcohol and drug use, and immigration status. Sensitive data elements are defined as those that have a high potential for harm or embarrassment to the respondent if his/her identity were somehow discovered. Although CHIS takes every possible precaution to protect the identity of survey respondents, due to the deductive disclosure risk inherent in distributing public-use data files it is impossible to guarantee that disclosure risk has been completely eliminated. Because of the small but continuing risk of disclosure and the risk of harm to the respondent should such information be disclosed, highly sensitive CHIS data elements are withheld from public release. These sensitive data elements are retained in the confidential source data files in the DAC to facilitate legitimate research uses of these data in a secure environment that protects the confidentiality of CHIS respondents.

2. DAC Structure and Policy

a. CHIS Principal Investigator

The CHIS Principal Investigator (PI) bears overall responsibility for protecting the privacy and confidentiality of CHIS respondents and may make CHIS data available under the authority of human subject protection committees. DAC policies and procedures for researcher access to confidential CHIS data are contained within this document. DAC policies and procedures are developed under the direction of the CHIS PI by the CHIS Director and other members of the CHIS team in collaboration with the Data Disclosure Advisory Committee. Because the DAC provides access to confidential CHIS data, it operates under the oversight authority of the UCLA Office for the Protection of Research Subjects (OPRS) and the State of California's Committee for the Protection of Human Subjects (CPHS).

In addition to OPRS and CPHS, there are two committees involved in the oversight of DAC operations. The CHIS Data Disclosure Advisory Committee provides expert advice to the CHIS PI on confidentiality policies and procedures, including for the DAC, and the CHIS Data Disclosure Review Committee provides expert review and recommendations to the CHIS PI on researcher requests to access confidential data through the DAC.

b. CHIS Data Disclosure Advisory Committee

The CHIS Data Disclosure Advisory Committee (DDAC) draws on the expertise of individuals with an understanding of privacy and human subjects protection issues. The DDAC provides guidance on confidentiality policies proposed by the UCLA CHIS staff or the CHIS Data Disclosure Review Committee, and evaluates the acceptability of disclosure risk associated with various disclosure limitation processes and procedures.

The DDAC is composed of representatives of CHIS partner organizations and agencies, CHIS Advisory Board members, and county health agencies. Membership is updated annually and consists of the following members:

- One representative from the California Department of Public Health
- Director of UCLA Center for Health Policy Research
- CHIS Director
- One representative from the Public Health Institute
- One representative from the California Conference of Local Health Officers
- One representative from the Southern California Public Health Association
- One representative from the California Pan-Ethnic Health Network
- One representative from the National Cancer Institute
- One representative from the California State Rural Health Association
- CHIS Data Access and Confidentiality Manager

The DDAC generally meets at least annually and on an as-needed basis when issues arise. Meetings are conducted via conference calls or in-person. CHIS staff develop meeting agendas in consultation with the DDAC chairperson. CHIS staff are responsible for coordinating the meetings, developing meeting materials, disseminating meeting materials to DDAC members prior to the meetings, and for providing summaries of meeting actions and resolutions following the meetings.

c. CHIS Data Disclosure Review Committee

The CHIS Data Disclosure Review Committee (DDRC) is responsible for implementing the confidentiality policies adopted by the CHIS PI and approved by OPRS and CPHS. The DDRC's main tasks include: review of data files, data products, and data requests to ensure that CHIS respondents' privacy and confidentiality are not violated; review of CHIS variables and recommended confidentiality and sensitivity levels; recommendations on disclosure limitation techniques for the public-use files; and review of applications for research use of data through the Data Access Center. The DDRC recommends decisions to the UCLA CHIS PI for final approval.

The DDRC consists of the following members:

- CHIS Director
- One representative of the California Department of Public Health
- One representative of the Public Health Institute
- CHIS Research and Survey Support Manager
- UCLA CHPR Data Access and Confidentiality Manager
- UCLA CHPR Director for Statistical Support & Programming

The DDRC meets on a bi-weekly basis, or as needed. CHIS staff are responsible for coordinating the meetings, preparing necessary meeting materials, and developing meeting minutes and recommendations.

In reviewing researcher applications for access to confidential CHIS data through the DAC, each participating DDRC member has one vote. Any member who has a conflict of interest with a request should recuse him/herself from the discussion and decision on that request. The DDRC may decide to appoint a primary reviewer to screen requests for access to confidential data.

3. Procedures to Access CHIS Confidential Data

a. User application process

Researchers seeking access to confidential CHIS data through the DAC must submit to the DDRC an application that includes a research proposal. This proposal must be submitted at least one week prior to the DDRC meeting to ensure review at the next regularly scheduled meeting. Research applications to use confidential CHIS data do not require approval or exemption from a human subjects institutional review board (IRB). The CHIS PI has obtained approval from the UCLA South General IRB to conduct analyses of confidential CHIS data through the DAC, including providing such analyses to other researchers (approval # here).

The application to access confidential CHIS data at the DAC is required to include the following information:

1. Cover letter
2. DAC application form (containing project title, summary, personal and organizational information, funding source, anticipated DAC project dates, software requirements, and publication plans)
3. Current biographical sketch or résumé
4. A description of the research study that includes project purpose or aims, research questions or hypotheses, methodology, statistical analysis plans, and publication plans (Portions of doctoral dissertation proposals or grant applications with appropriate modifications may suffice for the research proposal. DAC staff are available for consultation on the development of research proposals.)
5. A complete list of the CHIS variables requested
6. A detailed description of any user-supplied data files to be merged with California Health Interview Survey data, including documentation, file layout, number of records, and restrictions on the use of the data
7. Research projects applications submitted to the DAC by undergraduate or graduate students must show evidence of faculty sponsorship (A brief letter from the faculty sponsor stating that he/she has reviewed and approved the research proposal will meet this requirement.)

b. DDRC review of DAC application

Upon receipt of a fully completed application, the DAC Manager will send the requestor a dated acknowledgement of receipt. The DDRC will review the application at its next scheduled committee meeting and make a recommendation to the CHIS PI for approval, rejection, or request for further information. All available Committee members are expected to review the application. In cases of a conflict of interest, the involved Committee member should recuse him/herself as noted above.

The CHIS DDRC will use the following criteria to review and evaluate projects:

1. Feasibility of the project, that is, whether it is possible for the proposed research to be conducted with the available information.

2. Risk of disclosure of confidential information, that is, whether the analysis can be conducted without compromising the confidentiality promised to CHIS respondents.

3. Whether the proposed project is consistent with the purpose of CHIS, that is, to conduct population-based research on the health and health care needs of people in California to the benefit of that population.

4. Whether the variables requested match the list submitted to and approved by the applicant's IRB, if applicable.

c. CHIS Principal Investigator approval

The DDRC will make a recommendation to the CHIS PI. The CHIS PI will notify the requestor of the decision to accept or reject the request, or to request additional information, generally within 20 working days from the receipt of the application. The acceptance letter will state that the approval should not be interpreted as an endorsement of the project. The approval only constitutes a judgment that the proposed use of the CHIS confidential data meets the minimum criteria listed above. Following project acceptance, DAC staff will coordinate payment and access options with the researcher.

Once an applicant's project is approved by the CHIS PI for access to confidential data, the researcher must input an entry on the CHIS Research Clearinghouse at www.chis.ucla.edu/rc/. The Clearinghouse shares information about research studies using CHIS data, whether confidential or public-use data files. The amount of information that is publicly accessible is controlled by the researcher, but a basic entry — with research name, institutional or organizational affiliation, contact information, title and purpose of the study — must be provided and will be visible to other visitors.

d. Approval expiration

All approved DAC projects will expire two (2) years after the date of DDRC project approval. Expired projects must complete the DAC Project Renewal form (available on the DAC section of the CHIS website).

e. Expansion of approved projects

Projects that have previously been approved to access CHIS confidential data and wish to expand the original project to use data from another CHIS cycle may submit an expedited "Project Expansion" application (available on the DAC section of the CHIS website). Expanded projects require a new or modified IRB approval or exemption, if applicable, that clearly indicates the addition of the new data source. Please note that the requested variable list for the project expansion must match the approved variable list from the originally approved project; if the variable lists do not match, a new DAC application is required.

f. Required confidentiality assurances

Researchers whose applications are approved by the CHIS PI will be required to sign a Nondisclosure Affidavit and a CHIS Research Clearinghouse entry (See Appendix A) as a condition of accessing data

through the Data Access Center. The user will be held to the terms and conditions of the agreement. Breaching the terms and conditions of the Nondisclosure Affidavit will result in immediate termination of access to the confidential data files.

g. Researcher-supplied data

The Data Access Center will allow researchers to supply their own data to be merged with CHIS data. The supplied data may consist of proprietary data collected and owned by the user, or publicly available data obtained by the user. Users must provide DAC staff with adequate documentation of any data proposed for merging with CHIS data. The users are responsible for interacting with DAC staff to ensure that the data can be merged and that the formats are consistent.

h. Options for accessing confidential CHIS data

Researchers with approved projects (see "User application process" above) may be granted access to the CHIS confidential data. However, researchers are not permitted to physically access confidential CHIS data files in the DAC. Fees are charged on an hourly basis for DAC access and cost information is provided in the "DAC Fact Sheet." Approved research projects have two options available for conducting the analysis.

1. Remote indirect access. This method allows researchers to write their own statistical code (in SAS, STATA, or SPSS format) and send the code to DAC staff via email. Once the code is received by DAC staff, it is run by DAC staff on the confidential data files maintained within the DAC. Programming output is reviewed for disclosure risk by DAC staff (see guidelines for disclosure review below); if no risk is detected, the output is emailed back to the researcher. This option is facilitated by "dummy" data files made available to researchers for download at no cost through the CHIS website.

   The "dummy" data files allow researchers to write their own code and run it on the "dummy" data to ensure that the code is error-free and produces the results in the expected format. The "dummy" data files contain virtually every variable that is in the confidential data file. In addition, the sample sizes for these data files are identical to those of the adult, adolescent, and child files. Values in the dummy data files are scrambled, but the unweighted frequency distribution of the source file variable is retained in the corresponding dummy data file variable. The inter-variable relationships are generally maintained, but may not be for every variable for every respondent. The data may not be used to derive population estimates or associations between variables. The geographic data contained in the "dummy" files were generated randomly, but county level frequencies are similar to those in the confidential data file.

2. Programming services. In this option, researchers work with the UCLA-CHPR SSP staff to develop a research plan for their approved project. The SSP staff write the statistical software code and run the code on the confidential data within the DAC. SSP staff may assist in the interpretation of the statistical results and communicate results, including statistical output that does not pose a disclosure risk, to the researcher.

Prospective researchers should contact the DAC staff well in advance of their planned use of the DAC to ensure that their research proposal is reviewed and approved and that all necessary data files, computer hardware and software are available.

i. Disclosure risk review methods for data output

The California Health Interview Survey (CHIS) does not collect directly identifiable information, such as full name or social security number, from survey respondents. During survey administration, CHIS collects from respondents potentially identifiable information, such as exact date of birth. This information is not delivered to UCLA-CHPR by the CHIS data collection contractor, Westat. In the case of respondent date of birth, UCLA-CHPR receives only month and year of birth from the data collection contractor. Additionally, respondent contact information (such as telephone number and first name) is recorded by the data collection contractor and then separated from the survey data that is delivered to UCLA-CHPR. This contact information is retained by the data collection contractor for a specified period of time and then destroyed; it is never delivered to UCLA-CHPR.

UCLA-CHPR does receive specific geographic location (i.e., latitude and longitude, census tract block group), which may identify a respondent. Due to the potential risk to respondent re-identification posed by these variables, they are stripped from the main CHIS data file and maintained in a restricted access folder within the DAC. Data files containing CHIS respondent latitude and longitude cannot leave the DAC without the written approval of the CPHS. There are a number of other variables that, in combination with other variables, may also pose a risk of identifiability. In order to reduce the risk of disclosing a respondent's identity, CHIS conducts a disclosure risk analysis and assigns an identifiability rank to every variable.

Identifiability analysis performed on the CHIS data set divides all data elements into four categories: 1) Highly Identifiable Variables, which are high-risk, detailed demographic or geographic variables that are generally considered indirect identifiers (e.g. birth date, zip code),; 2) Key Variables, which are demographic characteristics (e.g. age, race, gender, etc.) that could identify an individual only in combination with other data; 3) Moderately Identifiable Variables, which have some identifying information (e.g., highly visible characteristics, or information which could be used to re-identify an individual in limited circumstances, particularly in smaller geographic areas); and 4) other variables that pose little or no risk of respondent re-identification.

1. Highly Identifiable Variables include, but are not limited to:
    a. Month, year of birth
    b. Detailed race/ethnicity and tribal affiliation
    c. Detailed country of birth.
    d. Person and household identifiers
    e. Variables describing relationship of household members
    f. Verbatim responses
    g. Stratum, county
    h. Zip code
    i. Census tract block group, latitude/longitude

2. Key Variables include, but are not limited to:
    a. Age
    b. Race
    c. Gender
    d. Tribal enrollment (Y/N)
    e. Specific cancer type
    f. Service in armed forces
    g. Income/alimony/social security
    h. Citizenship
    i. Years in U.S.

j. Specific industry/occupation
k. Marital status
l. Education
m. Household size, type, composition

3. Moderately Identifiable Variables include, but are not limited to:
    a. General health conditions
    b. Country of Birth, Years in U.S. in broader categories
    c. Language Spoken at Home
    d. Occupation/Industry in broader categories
    e. Public Program Insurance Coverage (Medicare, Medi-Cal, Healthy Families)
    f. Public Program Participation (WIC, SSI, GA, public housing subsidies, food stamps, etc.)
    g. Work Status
    h. Income/Alimony top/bottom coded
    i. Height/weight top/bottom coded
    j. Rural/Urban Geographic Area

CHIS identifiability analysis is additionally conducted mindful of the fact that even a broad code structure with large categories might still represent a disclosure risk if it characterizes only a very small number of study participants. In further mitigating this risk two considerations are paramount:

1. will the classification or information permit the isolation of respondents - does it produce "outliers"? and
2. is this information likely to be found in an external data source that also contains direct identifiers?

Research projects that conduct analyses of confidential CHIS data may have the output emailed to them by CHIS or SSP staff as described above. Before the output is sent outside of the DAC, the output must be reviewed to ensure that the output does not pose a risk of respondent re-identification. The following guidelines have been established for disclosure risk review by CHIS and SSP staff:

- Record-level information from CHIS confidential data files may only be reviewed within the DAC and must be done by CHIS or SSP staff. All output produced from CHIS confidential data files will be carefully reviewed to avoid disclosure risk before it is released outside of the DAC.
- Factors considered in disclosure review include geographic level, type of analyses, whether identifiable variables are included in the analysis, and whether sensitive variables are included in the analyses.
- No output that could potentially lead to the re-identification of a respondent, either directly or inferentially (e.g., geocode data, tables with small cells, or estimates run for individual zip codes), may be removed from the DAC under any circumstances.
- Regression analyses or linear models require review *only* when a geographic variable is one of the dependent variables. Frequencies and cross-tabulations will be reviewed as follows:
    - Analysis involving state-level or Los Angeles County (whole county) geographic areas: All unweighted and weighted frequencies where N<3 will be carefully reviewed and cells will be suppressed if the analysis includes:
        - *a sensitive variable (coded 1) and any two highly or key identifying variables (coded 1 or 2)* [1]
        - *any three highly or key identifying variables (coded 1 or 2).*

[1] Sensitivity and identifiability rankings are generated for every CHIS variable and assigned a score from 1 (highest risk) to 4 (lowest risk). The approach and procedures for assessing sensitivity and identifiability are described in detail in the *CHIS Confidentiality Manual.*

    - Analysis at the stratum level: All weighted and unweighted frequencies should be suppressed if N<3 and if the analysis includes:
        - *a sensitive variable (coded 1) and any identifying variable (coded 1 or 2)*
        - *a highly or key identifying variable (coded 1 or 2) and any other identifying variable (coded 1, 2, or 3)*
- Standard exceptions to the suppression of small cells
    - Univariate frequencies at the state level.
    - Small cells for "Other" or "Skipped" or "Don't Know" categories.
    - Cross-tabulations that include *identifying variables coded 3* and *no sensitive variables.*
- Cell suppression rules for cross tabulations
    - If one cell is eliminated, a complementary suppression must also be made.
    - If the output is a 2 x 2 table, the researcher will get only one row and one column variable.
    - If it is a 3 x 3 or more and any small cells exist, the reviewer must block at least two other cells so that two cells in each row and two cells in each column are blocked including the offending cell. Programmers must also check associated percentages and cumulative frequencies to ensure that these columns do not disclose the blocked cell.
    - In any two- or three-way table, all cases of any row or column should not reside in a single cell.
- Types of information requiring special approval from the Data Access and Confidentiality Manager
    - Unweighted frequencies that do not meet the cell suppression guidelines.
    - Estimates run on sub-stratum geographical areas, i.e., by aggregated zip codes or for certain counties that comprise part of a stratum.
    - Analyses that include highly sensitive variables.

Any questions about the appropriate release of data output should be directed to the DAC Manager.

j. Access to confidential CHIS data for research by UCLA-CHPR employees

This section describes access to confidential CHIS data by CHIS and UCLA-CHPR SSP staff for their own research purposes. As noted in the *Overview of DAC access & functions for research* in Section 1 of this document, there are only two groups of UCLA-CHPR employees that are allowed direct physical access to confidential CHIS data files: designated CHIS staff, and designated Statistical Support and Programming (SSP) staff.

Designated CHIS staff. A list of CHIS staff who are permitted direct access to confidential data files is maintained by the Data Access and Confidentiality Manager. Only those CHIS staff who are named on this list, which must be approved by the CHIS PI and CHIS Director, will be allowed direct access to confidential data files. The criterion for being so designated is that direct access to confidential CHIS data files is required as part of their staff position.

Designated UCLA-CHPR SSP staff. A list of UCLA-CHPR SSP staff who are permitted direct access to confidential data files will be developed and maintained by the Data Access and Confidentiality Manager. Only those UCLA-CHPR SSP staff who are named on this list, which must be approved by the CHIS PI and UCLA-CHPR Associate Director for Statistical Support, will be allowed direct access to confidential data files. The criterion for being so designated is that direct access to confidential CHIS data files is required as part of their staff position.

Designated staff are trained as researchers, conduct administrative analyses or research using CHIS data, and have specific administrative or research activities as explicit functions of their position. The guiding principle for staff access to confidential CHIS data is that all analyses must be conducted in accord with the policies set forth in this document and the terms and conditions of the signed nondisclosure affidavit. Any collaboration between designated staff and external researchers cannot be conducted to confer an advantage to access confidential CHIS data that the external researcher would otherwise not have.

Designated CHIS and SSP staff may directly access confidential CHIS data in the DAC for their own research projects provided that they have followed all other required protocols to access the data (IRB submission, DAC application, DDRC review, etc.) and have secured approval from the CHIS PI to proceed with the proposed research. DAC and IRB applications must clearly identify collaborators on proposed research projects. The output of analyses by CHIS staff for their own research purposes must be reviewed by another designated UCLA-CHPR SSP staff person; such output of analyses by UCLA-CHPR SSP staff for their own research purposes must be reviewed by a designated CHIS staff person before such output is removed or transmitted outside of the DAC to ensure that the output does not pose a risk of respondent re-identification.

4. DAC Network Security

a. Network infrastructure

1. Servers
    a. Internal LAN—The DAC server base consists of one Windows 2003 domain controller, one Windows 2008 file server, one management server, one software installation server and one workstation configured to perform hard drive backups of the DAC data.
    b. External LAN—Three Center servers have access to the secure DAC network; all unnecessary services have been disabled on Internet facing servers that need to access the DAC network for the purpose of maintenance.
    c. Additionally, one Windows 2003 SSH2 secure file transfer server has indirect access to the secure DAC network; it has no direct access to the DAC or Center networks, but has its own network and a drop-off network that is manually turned on and off when data is delivered to the DAC.

2. Workstations and printers
    a. There are 18 DAC Windows XP workstations, with one supervised system used to copy programs/results to and from the DAC file server.
    b. There are 2 Protected Health Information (PHI) workstations located in a separate secured room within the DAC. Please note that CHIS confidential data is <u>not</u> maintained or accessible through the PHI workstations.
    c. There are 11 Center Windows XP workstations located in the DAC; staff uses a 2-port KVM switch to access either Center or DAC workstations.
    d. There are 3 network printers located in the DAC, one is connected to the DAC network, one is connected to the PHI network and one is connected to the Center network.

3. Switch configuration
    a. The Center for Health Policy Research primary LAN segment consists of a stack of four Enterasys C2G124-48 1.0GB 48-port switches. The stack is connected to the Internet via a Watchguard Firebox X 1000 firewall, providing LAN and Internet service to the CHPR domain. A 32-port secure vlan segment resides on the third switch of the Enterasys stack.

Two entirely segregated confidential data networks reside on the secure vlan: The Data Access Center (DAC) and the PHI data network. Any workstations that connect to either of those segregated networks also reside on the secure vlan. The secure vlan has no ingress or egress with the remainder of stack; therefore, the DAC/PHI network segment is completely isolated and has no access to the Internet. Additionally the DAC and PHI networks each have their own domain and are logically separated from each other via different network subnet masks and unique IPSEC policies. Every network port on the DAC vlan segment is assigned to a unique DAC workstation via MAC address locking on the switch; the workstations cannot change ports and any foreign network device connecting to any of the DAC network ports will be denied access. There is no wireless access to any vlan segment on the 4-switch stack.

b. Redundancy

1. Backup equipment
   a. The DAC shares a backup server with CHPR. The server is connected to an 8-tape LTO4 robotic device and the DAC has three 800GB/1.6TB tapes dedicated solely to DAC backups. Full tape backups occur once a month and incremental backups occur daily. Backup Exec 12.5 is the software installed on the backup server. In addition to the LTO4, a single slot 160/320GB backup device is also connected to the backup server; approximately once every six weeks all DAC data will be backed up to this device and the tapes will be stored in a fireproofed safe located in the School of Public Health. Only the CHPR Director of Finance and the network security officer have access to this safe.
   b. An internal backup workstation is also implemented; it has two 750GB hard drives and the DAC data is fully backed up to hard drive every two weeks. Windows backup is used for the hard drive backups.

2. Uninterruptible power supplies
   a. APC Smart-UPS 2200XL is connected to the data server, domain controllers, management server and the backup workstation. During a power outage the runtime given that load will be approximately 25 minutes before sending the servers a network signal to shut down.
   b. APC Smart-UPS 3000XL is connected to (among others) 2 management servers and the backup server on the Center network. During a power outage the runtime given that load will be approximately 35 minutes before sending the servers a network signal to shut down.

3. Hard drives
   a. The DAC data server has two 160GB SATA hard drives RAID 1 mirrored for the operating system partition and three 750GB SATA hard drives in a RAID 5 configuration for the data partition; total usable data space is 1.5TB.

c. Facility security

1. Physical Security
   a. DAC staff area and workstations
      i. The door to the DAC is always locked and the door has an automatic door closer. Authorized UCLA CHPR staff is provided with a photo-ID card that provides monitored key-card access to the electronic security lock at the DAC.

ii. The doors use swipe pads common to the rest of the suite and can only be opened by authorized employees and authorized building personnel.
iii. All DAC user workstations have all physical/logical removable media disabled, including floppy, CD-ROM and all USB, serial and parallel ports. The BIOS setup is password protected and the CPU chassis is locked using a heavy-duty combination padlock.
iv. The supervised media station is the only DAC network connected workstation that has floppy, CD/DVD and Zip access. Its use is monitored by the DAC Manager.

b. DAC data server and backup devices
   i. The room that houses the DAC data server is in a secure communications room with access limited to the director of the Center for Health Policy Research, the Director of Finance, the network security officer and his assistant and three building engineers. The DAC data server is itself locked and resides inside of a securely locked server cabinet; all of the entry points on the cabinet are locked and the hinge covers are built into the side panels. Key access to the cabinet is limited to the director of the Center for Health Policy Research, the Director of Finance and the network security officer.
   ii. The 8-tape LTO4 also resides in the secured server cabinet and the front panel is password protected disallowing the removal of the tapes. An additional 8-tape 160/320GB robotic device is also in stalled in the cabinet and will be used as a fail-safe backup device to the DAC and will be used to backup inbound data from the Center's SSH server—also housed in the secure data cabinet.

2. Operating Systems and Logical Security
   a. Encryption methods—Networks, servers, workstations and off-network access
      i. Network—Encryption is provided via Windows 2003/2008 IPSEC policies that separate the DAC data server and clients from the PHI server and clients. Additionally, the policies ensure that rogue network devices cannot communicate with any part of the DAC network. MAC address locking of the secure vlan segment of the switch further prevents communications with any part of the network. Conversely, any DAC workstation that is connected to a network other than the DAC will have no ability to communicate with that network or its clients.
      ii. Servers—To ensure the highest possible chance of data recovery in the event of a catastrophic system failure, the DAC file server is not encrypted. Previous experiments with server encryption have also shown that it interferes with some software that depends on access to file shares.
      iii. Workstations—While no data is to be copied to local workstations in the DAC, some software generates local temporary datasets while accessing network drives. To remedy this situation all hard drives on all workstations are fully encrypted using PointSec encryption software. In the event that one of the locked workstations is broken into and the hard drive is removed, it will be totally unreadable without the security key. In addition to software based encryption, all users in the DAC have limited access accounts that prevents them from accessing sensitive system security settings and prevents them from installing system level software on their workstations.
      iv. Off Network Access—While the DAC is a closed loop network, it is necessary to access the DAC management server to provide system updates, anti-virus definition updates, account management and software installations. Two servers and one workstation on the Center's domain have this type of access; all of these systems have IPSEC policies used for their communications with the DAC, can only communicate with the DAC management server and they all have local group policies that prevent either console or network access to anyone except the Center's network security officer. The shared

backup server, which is a member of the Center domain, also has a DAC network address and is only allowed to connect to the DAC file sever via IPSEC policies; all data backed up from the DAC server goes straight to the LTO4 tape drive via remote backup client software. As an additional protective measure, on the Center network, the backup server is only allowed to communicate with file servers is backing up and 2 management servers.

3. User Security Policies and Procedures
   a. External Access of CHIS Data
      i. CHIS does not allow researchers to access confidential CHIS data from computers or workstations outside the DAC. All access to the confidential data files must be conducted by CHIS staff or UCLA-CHPR Programming staff on-site in the DAC.

   b. User Authorization
      i. Currently staff receives an 8-digit non-dictionary password created by the network security officer to ensure password quality; by the end of June 2009 all users will be required to create their own strong password and change it every eight weeks.
      ii. There are no common or group accounts that can be accessed using shared passwords.
      iii. Domain network credentials are required for secure logons and network access to shares on the file server; there are no local accounts on any DAC workstations.
      iv. Printouts can only be performed on a single printer supervised by the Data Access Center Manager. Copying of files onto or off of the DAC network can only be performed from a single management workstation supervised by the Data Access Center Manager.
      v. All printouts and electronic output are subject to a Disclosure Review Process, where all output is reviewed by DAC senior staff for any information that presents a risk of disclosure or possible respondent identification.

   c. Access Rights to Data Files—When research project accounts are created, assigned staff is given specific access rights to various directories on the DAC server. These access rights are summarized below:
      i. Staff working on research projects is restricted to use the custom data sets for specific projects, located in the Client's directory with the researcher's name and an assigned DAC project number. These custom data sets include the elements approved by the DDRC.
      ii. Only those programmers and/or CHIS staff responsible for data preparation and quality control have access to the source data sets of the CHIS confidential files, which are located in separate directories not accessible to guest researchers.
      iii. Only the network security officer has administrative access to the operating system on either the client or server computers.

   d. Technical Controls
      i. Screensavers come on after 10 minutes of non-use, locking the desktop and forcing the user to re-authenticate; this is a group policy setting and cannot be changed.
      ii. No remembered passwords or auto-logon routines are permitted on DAC workstations.
      iii. Only the network security officer can install software on the DAC server or workstations.

Glossary

CHIS	California Health Interview Survey
CPHS	Committee for the Protection of Human Subjects, the State of California's IRB which has oversight authority for all research conducted by State agencies or conducted with funding under contracts with State agencies. CHIS is funded, in part, by several State contracts and thus is under the jurisdiction of CPHS, as well as the UCLA SGIRB
DAC	Data Access Center, a secure data analysis facility operated by the UCLA Center for Health Policy Research
DDAC	Data Disclosure Advisory Committee, a committee appointed by the CHIS PI to provide expert advice on confidentiality policies and procedures for the DAC and for CHIS
DDRC	Data Disclosure Review Committee, a committee appointed by the CHIS PI to provide expert review and recommendations on researcher applications to access confidential data through the DAC
IRB	Institutional Review Board, a human subjects protection committee
OHRP	Office for Human Research Protections, a unit within the federal Department of Health and Human Services
OPRS	UCLA Office for the Protection of Research Subjects, the office that manages all human subjects research at UCLA
PI	Principal Investigator, the person who has ultimate responsibility for the conduct of CHIS and thus the protection of confidentiality and privacy of CHIS respondents
SGIRB	South General Institutional Review Board, the UCLA IRB with jurisdiction over CHIS. Because CHIS is conducted hy a UCLA organizational unit and lead by a UCLA faculty member, CHIS is under the jurisdiction of UCLA SGIRB, as well as the CPHS
SSP	Statistical Support and Programming, a department of the UCLA Center for Health Policy Research
UCLA-CHPR	UCLA Center for Health Policy Research

CHIS Data File Delivery Protocol

This document specifies the protocol for preparing and removing confidential data files from the UCLA Center for Health Policy Research Data Access Center (DAC) for delivery to funders, local health departments, and Internet posting of public use files (PUFs). This protocol designates specific CHIS and Statistical Support and Programming (SSP) staff to conduct the various tasks associated with the data delivery process; if a designated CHIS or SSP staff member is not available, an alternate can be designated by either the CHIS or SSP director.

All elements of this protocol must be followed before data is removed from the DAC for delivery.

Summary of steps for data file delivery

1. Data delivery planning meeting
2. Data file request
3. Data file cut
4. Programmer review and verification
5. CHIS review and package assembly
6. CHIS leader package review and verification
7. Data file release
8. Delivery log

Detailed steps for data file delivery

1. **Data delivery planning meeting**—in order to plan the delivery of CHIS data files, the CHIS Research and Survey Support Manager (RSSM) will a schedule meeting with the CHIS Data Access & Confidentiality Manager (DACM) and the UCLA Center for Health Policy Research Grants and Development Manager (GDM). Successive meetings will be scheduled as needed to update file requests and status. This team will develop a list of all data delivery recipients and discuss the following elements necessary to initiate delivery of data files for intended recipients (**Document: Data Delivery Planning.xls)**.
    a. Recipient
    b. Recipient type (PUF, Funder, LHD, other)
    c. Target date of delivery
    d. Age group (Adult, Teen, Child)
    e. Confidential data requested? (yes/no)
    f. Data Sharing Agreement (DSA) required? (yes/no)
        i. Data Sharing Agreement (DSA) complete? (yes/no)

2. **Data file request**—following the planning meeting, the RSSM will initiate the file delivery process for each file recipient. The RSSM will complete Part I of the File Request form, which provides general information about the delivery; a separate form must be completed for each recipient. Upon completion of Part I, the RSSM will send the form to the DACM to develop the data file variable contents ("specs") and the location of the specs file. The specs will be completed by the DACM in collaboration with the DAC coordinator. The specs must contain the variable name, variable label, and sensitivity and identifiability rankings for each variable.[1] When

[1] The sensitivity and identifiability rankings are conducted as part of the risk disclosure review and described in detail in the *CHIS Confidentiality Manual.*

the specs are complete, the DACM will complete Part II of the File Request form and send it back to the RSSM. The DACM will identify any special variables or other unique information about the file in the "notes" section of the form. If required, **a copy of the fully executed data sharing agreement or the data custodian agreement (for local health dept. files)** must be provided at that time. The specs will be checked and verified by the RSSM. In order to insure the delivery of variables in accordance with the data sharing agreement, the RSSM will sort and flag potentially sensitive and/or sub-state geographic variables. Questions or concerns regarding the appropriateness of these variables in the specifications will be discussed by the RSSM with the DACM. The RSSM will update the data delivery database to document the variables for delivery to the file recipient. The Data File Request form includes the following (**document: Data File Request.pdf**):

a. Recipient organization
b. Recipient type (PUF, funder, LHD, other)
c. CHIS data year(s) requested
d. File age group(s) (Adult, Teen, Child)
e. Data file formats (SAS, SPSS, STATA)
f. Universe (Statewide, Stratum, Other)
g. Spec file name and location
h. Notes to identify special variables or unique aspects of the file

3. **File cut**—following completion of the File Request form and the specs file, the RSSM will send a copy of the form and the database to the Programming Team supervisor. The Programming Team supervisor will review the form and specs and consult the RSSM if necessary. The supervisor will then assign a member of the programming team to cut the data file and generate accompanying label, format, and proc format files following the information included in the file request. The programmer will also generate relevant documentation (i.e. data dictionary) for inclusion in the data delivery. When all of the necessary elements have been generated, the programmer will place the files in a delivery folder on the secure DAC network. The programmer will produce a data summary from a SAS macro directly from the datafile. This "Data File Summary" report (in Excel format) will be used to verify the number of variables and observations in the data file and be placed in the delivery folder on the DAC network. When all of the files and the data summary report are complete, the programmer will notify the Programming Team Supervisor. The Data File Summary report includes the following **(document: Data File Summary.xls):**
    a. Recipient
    b. Date files produced
    c. CHIS data years
    d. Universe (Statewide, Local County, Other)
    e. Details for each ATC file cut, including:
        i. # of variables
        ii. # of observations
        iii. File names (data set, label, format, proc format, dictionary) and location on DAC server
        iv. Relevant notes

4. **Programming Review and Verification**—after the files have been prepared and the Data File Summary form completed, the Programming Team Supervisor must review and verify the content of the data file(s) using the **data file request** and **data file summary** forms. If any problems are encountered, the Supervisor will consult with other CHIS and/or programming team members to resolve the problem. When the files are accurate, the Programming Team Supervisor will complete and sign the release authorization form (**Document: Programmer_Authorization Data Release.pdf**) that includes a checklist for the following file elements:

a. Each file (ATC) and version (SAS, SPSS, STATA) opened and checked for functionality
b. Number of variables match file request
c. Number of observations match file request
d. Files do NOT contain LAT/LONG or Census tract block group
e. Supporting documentation produced (data dictionary) and consistent with specifications

The programming team supervisor will then notify the RSSM that the files are ready for release to the CHIS team, send a completed copy of the Data File Summary form, send the completed and signed Programmer Authorization for Data File Release form, and identify the DAC folder location for the delivery contents.

5. **CHIS Review and Package Assembly—**after receiving notice from the programming team supervisor that the files are ready for review, the RSSM will ensure that all necessary forms have been completed (**Data Delivery Request form, Data Delivery Summary form, Programmer Authorization for Data File Release form, and copy of the data sharing agreement/data custodian agreement).** The RSSM will instruct a CHIS team member to format the data dictionaries and create a data delivery cover letter for the intended recipient. The CHIS team member will also enter the DAC, access the files for delivery, zip the files and burn them on to a password protected CD**.** The CHIS team member will deliver the documentation and password protected CD(s) to the RSSM and notifies him/her that the zipped are ready for review and verification within the DAC.

6. **Package Review and Verification**—the RSSM must review and verify the accuracy of the data file(s) intended for delivery within the DAC. The RSSM will access the CD within the DAC and copy all files unto the DAC server for review. S/he will then complete and sign the release authorization form (**Document: CHIS_Authorization Data Release.pdf**) that includes a checklist for the following file elements:
   a. Each file (ATC) and version (SAS, SPSS, STATA) opened and checked for functionality
   b. Password verified on all files
   c. The number of variables (# VARS) match file request
   d. The number of observations (# OBS) match file request
   e. Files do NOT contain LAT, LONG or Census Block/Tract
   f. Supporting documentation included (data dictionary)

7. **File Delivery**—a CHIS team member will deliver the CD(s), the cover letter and the documentation to the CHIS Director for final review. The CHIS team member will then prepare the FedEx package and deliver the data files and signed cover letter to the intended recipient. The CHIS team member will update the CHIS data delivery log (see #8 below), email the password to the CHIS Director, CC all persons on the cover letter, and notify the intended file recipients that the package is on its way.

8. **Delivery Log**—a record of all data file deliveries will be maintained under the supervision of the RSSM. The log will record all pertinent elements of the data file delivery for each recipient, including the files delivered, date of delivery, file contents (variables), and name and contact information for the recipient. The delivery log will be maintained on a network drive with regularly scheduled back-up. The RSSM will also be responsible for keeping an electronic folder containing the completed forms associated with each recipient in a read-only format.

PROGRAMMER AUTHORIZATION FOR DATA FILE RELEASE

The California Health Interview Survey (CHIS) is bound by promises made to respondents, by California law, and by University and government human subject protection committees to assure that no personal information is released in a form that identifies an individual without the consent of the person who supplied the information.

In order to protect against the unintentional release of identifiable, confidential, or sensitive data the "CHIS Data File Delivery" protocol must be followed any time data or data files will be copied off of the secure DAC network or transported out of the Data Access Center for any reason.

Data File Recipient: _____

Name of Programmer: _____

By checking the boxes below, I certify that I have conducted each task below to ensure that the data file(s) are accurate and consistent with the specifications and data delivery request.

- ☐ File(s) opened and function appropriately
- ☐ Number of variables match file request
- ☐ Number of observations match file request
- ☐ Number of observations match county fact sheet (LHD only)
- ☐ Files do **NOT** contain LAT/LONG or Census track Block group (CBLK)
- ☐ Supporting documentation matches specs

PROGRAMMING STAFF RESPONSIBLE INDIVIDUAL AUTHORIZATION

I the undersigned have verified all file contents for this delivery created by the PROGRAMMER specified above, reviewed all versions (Adult, Teen, and/or Child in SAS, SPSS, and/or STATA format), reported and verified the number of variables and observations, and certify that the files do not contain latitude/longitude, or Census tract block group. I certify that the file contents are appropriate for release from the secure DAC network and workspace, and hereby approve their release to CHIS Research and Survey Support Manager.

_____
PRINT NAME

_____
SIGNATURE DATE

UPDATED 5/19/2009

CHIS AUTHORIZATION FOR DATA FILE RELEASE

The California Health Interview Survey (CHIS) is bound by promises made to respondents, by California law, and by University and government human subject protection committees to assure that no personal information is released in a form that identifies an individual without the consent of the person who supplied the information.

In order to protect against the unintentional release of identifiable, confidential, or sensitive data the "CHIS Data File Delivery" protocol must be followed any time data or data files will be copied off of the secure DAC network or transported out of the Data Access Center for any reason.

Data File Recipient: _____

By checking the boxes below, I certify that I have conducted each task below to ensure that the data file(s) are accurate and consistent with the specifications and data delivery request.

- ☐ File(s) opened and function appropriately
- ☐ Number of variables match file request
- ☐ Number of observations match file request
- ☐ Number of observations match county fact sheet (LHD only)
- ☐ Files do **NOT** contain LAT/LONG or Census track Block group (CBLK)
- ☐ Supporting documentation matches specs

CHIS STAFF RESPONSIBLE INDIVIDUAL AUTHORIZATION

I the undersigned have reviewed all versions (Adult, Teen, and/or Child in SAS, SPSS, and/or STATA format) of all data file(s) provided by programming staff, verified that the information on the data delivery request and data delivery summary is consistent with the data file content, and certify that the files do not contain latitude/longitude, or Census tract block group. I certify that the file contents are appropriate for release from the secure DAC network and workspace and for delivery to the recipient specified above, and hereby approve their release.

_____
PRINT NAME

_____
DIGITAL SIGNATURE DATE

UPDATED 5/20/2009

CHIS Data Delivery	
Data File SUMMARY	
Your name:	
Date:	
Recipient (organization):	
CHIS data year/s:	
Universe	
ADULT	
# of Vars	
# of Obs	
Data file name	
Datacut program	
TEEN	
# of Vars	
# of Obs	
Data file name	
Datacut program	
CHILD	
# of Vars	
# of Obs	
Data file name	
Datacut program	
Notes:	

CHIS Data Delivery

Data File REQUEST

PART I, completed by: _____ Date: _____

Recipient (organization): _____

Recipient type

- ○ PUF
- ○ Funder
- ○ LHD
- ○ Other, specify: _____

CHIS data year/s: ☐ 2009 ☐ 2007 ☐ 2005 ☐ 2003 ☐ 2001

Age group/s: ☐ Adult ☐ Teen ☐ Child

Universe

- ○ Statewide
- ○ Stratum
- ○ Other, specify: _____

Data file format: ☐ SAS ☐ SPSS ☐ STATA

Spec file and location: _____

Field name: _____

PART II, completed by: _____

Date: _____

File summary

ADULT		TEEN		CHILD	
# Vars		# Vars		# Vars	
# Obs		# Obs		# Obs	

Notes: