NCHS Staff Manual on

Confidentiality

National Center for Health Statistics

Edward J. Sondik, Ph.D., *Director*

Jennifer H. Madans, Ph.D., *Acting Co-Deputy Director*

Michael H. Sadagursky, *Acting Co-Deputy Director*

Jennifer H. Madans, Ph.D., *Associate Director for Science*

Jennifer H. Madans, Ph.D., *Acting Associate Director for Planning, Budget, and Legislation*

Michael H. Sadagursky, *Associate Director for Management and Operations*

Lawrence H. Cox, Ph.D., *Associate Director for Research and Methodology*

Margot A. Palmer, *Director for Information Technology*

Margot A. Palmer, *Acting Director for Information Services*

Linda T. Bilheimer, Ph.D., *Associate Director for Analysis, Epidemiology, and Health Promotion*

Charles J. Rothwell, M.S., *Director for Vital Statistics*

Jane E. Sisk, Ph.D., *Director for Health Care Statistics*

Jane F. Gentleman, Ph.D., *Director for Health Interview Statistics*

Clifford L. Johnson, *Director for Health and Nutrition Examination Surveys*

Foreword

The *NCHS Staff Manual on Confidentiality* was originally published in July 1978 and reprinted in April 1980 and in August 1997. It was reissued in earlier years mainly to inform staff of changes in laws and regulations. In view of the many changes in technologies related to data handling and dissemination that have taken place in recent years, new procedures and policies have been developed requiring an extensive revision of the Manual.

The confidentiality of records is a matter of primary concern to the National Center for Health Statistics (NCHS). In order to elicit health information from the American people and from the health care providers through our surveys, we must be able to assure them that this information will be protected from the eyes and ears of all unauthorized persons. This means that we must have strong laws enabling us to protect these records, and that we must establish and follow procedures to give them such protection. This Manual states the Center's policies that implement Federal law and ensure that all confidential information will be fully protected. It should be viewed in unison with the NCHS data release policies addressing access to data and NCHS Research Ethics Review Board Requirements. *The NCHS Director retains the authority to allow exceptions to policies contained in this manual where there are unique or special circumstances.*

The Center is proud of its record in protecting its files from improper disclosures, and it is very important that we continue to do so. The continuing success of our work depends on it. Therefore, I am counting on every member of the staff of the Center, as well as those who work with NCHS, to keep a copy of this Manual handy, to be thoroughly familiar with its contents, and to abide by the policies in the manual carefully and conscientiously.

Edward J. Sondik, Ph.D.
Director

Contents

Foreword ii

1. Introduction 1

2. Legislative and Regulatory Background 1
   - 2.1 Section 308(d) of the Public Health Service Act 1
   - 2.2 Privacy Act of 1974 2
   - 2.3 Confidential Information Protection and Statistical Efficiency Act 2
   - 2.4 Freedom of Information Act 3
   - 2.5 Federal Law Governing Federal Employees' Behavior 3

3. Definitions 3

4. Employee Responsibilities 4
   - 4.1 Division and Office Directors 4
   - 4.2 Confidentiality Officer 4
   - 4.3 Supervisors' Responsibilities 4
   - 4.4 Individual Federal Employee's Responsibilities 5
   - 4.5 Contractors' and Agents' Responsibilities 5
   - 4.6 Collaborator's Responsibilities 5
   - 4.7 Administrative Officer's Responsibilities 5

5. NCHS Policies on Consent and Assurances of Confidentiality 5
   - 5.1 Consent 5
   - 5.2 Assurances of Confidentiality 6
   - 5.3 Responsibility for Formal Assurances of Confidentiality 7
   - 5.4 Data Collected Directly From Individuals or Establishments 7
   - 5.5 Data Collected From Another Organization 8
   - 5.6 Data Collected Over the Telephone 8
   - 5.7 Repository of Assurances 8

6. Treatment of Requests for Information Under Freedom of Information Act 9

7. The Protection of Confidential Records and Data Systems 9
   - 7.1 Physical Protection of Confidential Records 9
   - 7.2 Automated Data Processing Systems Security General 10

8. Authorized Disclosures 11
   - 8.1 Disclosure to the Parent Locator Service 11
   - 8.2 Disclosures Permitted by Section 308(d) of the Public Health Service Act 12

8.3 Disclosures Within NCHS 12
8.4 Disclosures Within the Department 12
8.5 Transfers of Data to Other Departments of the Federal Government 12
8.6 Special Cooperative or Contractual Arrangements 13

9. Avoiding Inadvertent Disclosures Through Release of Microdata 13
9.1 Problem 13
9.2 Rules 14
9.3 Restricted Access to Microdata Files With Identifiable Data 15

10. Avoiding Inadvertent Disclosures in Published Tabular Data 15
10.1 Types of Disclosure 15
10.2 Problem 15
10.3 Special Guidelines for Avoiding Disclosure 16
10.4 Evaluating a Disclosure Problem 16
10.5 Measures to Avoid Disclosure 17

11. Avoiding Disclosure in Other Types of Published Information 17

Appendixes

Appendix A. Requirements Relating to Confidentiality and Privacy in Data Collection and Data Processing Contracts 18
I. Purpose 18
II. Background 18
III. Policy 18
Safeguards for Individuals and Establishments Against Invations of Privacy 18

Appendix B. NCHS Nondisclosure Affidavit for Federal Employees 20

Appendix C. NCHS Nondisclosure Affidavit for Contractors 21

Appendix D. Confidentiality, Security, and Related Contact Persons 22

National Center for Health Statistics
Staff Manual on Confidentiality

1. Introduction

Confidentiality protection has many aspects. This manual attempts to deal with most of them. Information and rules are presented governing:

A. Legal requirements and penalties,
B. Employee's[1] responsibilities,
C. Promise of confidentiality to respondents,
D. Treatment of requests for information,
E. Physical protection of records,
F. Disclosures that may be permitted,
G. Avoidance of unintentional disclosures through published data,
H. Maintenance of confidentiality in the release of microdata, and
I. Requirements placed on contractors.

2. Legislative and Regulatory Background

The Health Services Research and Evaluation and Health Statistics Act of 1974 (P.L. 93–353) established NCHS in law. In doing so, it mandated that NCHS makes the information it collects available on as wide a basis as practicable. However, it placed a very important restriction on the manner in which this was to be accomplished by enjoining NCHS to strictly observe the assurances of confidentiality provided to its respondents. Making useful health statistics available to as many people as possible is very important, but it is equally important to do so in a manner that will not in any way harm the providers of these statistics.

Although it is a matter of principle, as well as good statistical practice, for the Center to maintain the confidentiality of records, a set of laws and regulations exists that requires and permits the Center to do so.

2.1 Section 308(d) of the Public Health Service Act (42 U.S.C. 242m(d))

This section provides the basic legal requirement for protecting the Center's records. It reads:

> ''No information, if an establishment or person supplying the information or described in it is identifiable, obtained in the course of activities undertaken or supported under section 242b, 242k, or 242l of this title may be used for any purpose other than the purpose for which it was supplied unless such establishment or person has consented (as determined under regulations of the Secretary) to its use for such other purpose; and in the case of information obtained in the course of health statistical or epidemiological activities under section 242b or 242k of this title, such information may not be published or released in other form if the particular establishment or person supplying the information or described in it is identifiable unless such establishment or person has consented (as determined under regulations of the Secretary) to its publication or release in other form.''

This section of the act is interpreted as follows: Whenever the Center requests information, it apprises the person or agency supplying the information as to the uses to be made of it.

The first clause of Section 308(d) guarantees that thereafter the Center will be limited to those uses so specified to the supplier.

[1]Wherever the word ''employees'' is used in this document, contractors, agents, fellows, and all other persons who have signed a nondisclosure agreement (''Appendix A or B'') are also included.

The second clause states that the Center may never release identifiable information (See Section 3. Definitions) without the advance, explicit approval of the person or establishment supplying the information or by the person or establishment described in the information.

Access to information in identifiable form may be granted *only* to staff of NCHS, its qualified agents, and those collaborators and other parties (including other Federal agencies) explicitly described in the survey consent statement, and may be employed by them only in activities *directly* aimed at achieving the specific purposes as conveyed to respondents.

2.2 Privacy Act of 1974 (5 U.S.C. 552a)

This act also provides for the confidential treatment of records of individuals that are maintained by a Federal agency that are retrieved by either the individual's name or some other identifier. This law also requires that such records in NCHS are to be protected from uses other than those purposes for which they were collected without the consent of the individual unless authorized by the Privacy Act. It further requires agencies to (1) collect only that information necessary to perform agency functions; (2) publish descriptions of data systems containing names or other direct identifiers (called ''systems of records'') so that the public can learn what identifiable records are maintained by the agency; (3) inform individuals at the time of data collection as to the legislative authority under which it is requested, whether the request is mandatory or voluntary, the consequences, if any, of nonresponse, and the purposes and uses to be made of the data; (4) maintain no records on how an individual exercises his rights under the first amendment except with special legal authorization; (5) with certain exceptions, permit individuals to examine records maintained about themselves and to challenge the accuracy of those records; (6) establish rules of conduct governing persons involved in collecting and maintaining records; and (7) establish appropriate administrative, technical, and physical safeguards to protect records. Employees of agencies and their contractors subject to the act who willfully disclose personal information contrary to the law, or who fail to give notice of a system of records, may be fined up to $5,000, and the agency may be sued for damages. Finally, the act places severe restrictions on the use of an individual's Social Security number, such that the Center is precluded from collecting and using them without the explicit consent of respondents.

The Department of Health and Human Services (DHHS) has allowed NCHS to have a ''K-4 exemption'' for its statistical systems, as permitted under the Privacy Act. This means that NCHS does not have to allow subjects of its data files to have access to the records about themselves in those files. This exception to Privacy Act requirements is permitted because NCHS does not have in its data files any records that are used in any direct way to affect the rights, benefits, or privileges of persons whose records exist in these files; rather, the files are used strictly for statistical and related purposes. The Center, however, must comply with all other requirements of the Privacy Act.

It must be stressed that while under the Privacy Act identifiable information may be released to a number of parties such as the General Accounting Office, either house of Congress, and courts, *the provisions of Section 308(d) of the Public Health Service Act, which are much more strict, would take precedence. Without the consent of respondents, identifiable information will not be shared with such parties.*

Regulations (*45 CFR Part 5b*) have been published by DHHS providing for implementation of the Privacy Act within this Department. All employees are bound to comply with these regulations.

2.3 Confidential Information Protection and Statistical Efficiency Act

(NO U.S. CODE LINK AVAILABLE AT PRESENT. Consult Kathy Moss.)

This legislation establishes strong standards for the protection of confidential data provided to Federal agencies for statistical purposes. This law requires that all data collected for statistical purposes under a pledge of confidentiality be used only for statistical purposes. As such, it covers all data collections currently undertaken by the Center. It also provides strong criminal penalties for unauthorized disclosure of confidential statistical information. Concerning fines and penalties, the act states:

> ''Whoever, being an officer, employee, or agent of an agency acquiring information for exclusively statistical purposes, . . . comes into possession of such information by reason of his or her being an officer, employee, or agent and, knowing that the disclosure of the specific information is prohibited under the provisions of this title, willfully discloses the information in any manner to a person or agency not entitled to receive it, shall be guilty of a class E felony and imprisoned for not more than 5 years, or fined not more than $250,000, or both.''

This Act does not diminish any confidentiality protection such as NCHS' 308(d) authority or those of the Privacy Act.

The Act also authorizes the designation of agents to perform statistical activities. These agents function under the supervision of NCHS employees and are subject to the same provisions of law with regard to confidentiality as an NCHS employee.

2.4 Freedom of Information Act (FOIA) (5 U.S.C. 552)

First passed in 1967 and amended most recently in 1996, this act requires Federal agencies to make their records available to persons who request them. While FOIA seeks to make government information more widely available, it does not undermine the privacy protection required under the laws just cited. Several kinds of records are specifically exempted from the disclosure requirements of the FOIA. Two exclusions provided in Section 552(b) of the act are of special relevance: Subsection (6) exempts ''personal and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy'' and Subsection (3) provides that matters ''specifically exempted from disclosure by statute'' are also excluded from the disclosure requirement. In the case of NCHS, the aforementioned Section 308(d) of the Public Health Service Act represents statutory protection. Thus no records that are collected under the Public Health Service Act and protected by Section 308(d) of that act are required by the FOIA to be released by anyone.

Regulations have been published by DHHS implementing FOIA.

In the event that NCHS staff or contractors receive a data request citing the FOIA, they are not to respond directly, but must refer the request to the NCHS Freedom of Information Coordinator immediately.

2.5 Federal Law Governing Federal Employees' Behavior (18 U.S.C. 1905)

This law includes the following provision, which is also relevant to the maintenance of confidentiality for NCHS records:

Disclosure of Confidential Information

> Whoever, being an officer or employee of the United States or any department or agency thereof, . . . ''publishes, divulges, discloses or makes known in any manner or to any extent not authorized by law any information coming to him in the course of his employment or official duties or by reason of any examination or investigation made by, or return, report or record made to or filed with, such department or agency or officer or employee thereof, which information relates to trade secrets, processes, operations, style of work, or apparatus, or to the identity, confidential statistical data amount or source of any income, profits, losses, or expenditures of any person, firm, partnership, corporation or association; or permits any income return or copy thereof or any book containing any abstract or particular thereof to be seen or examined by any person except as provided by law, shall be fined under this title, or imprisoned not more than one year, or both; and shall be removed from office or employment.''

3. Definitions

Throughout this document, certain key terms are used that warrant clear understanding. The reader is cautioned that present usage may not always coincide with usage by other agencies or entities.

Identifiable Information refers to information that can be used to establish individual or establishment identity, whether directly—using items such as name, address, or unique identifying number—or indirectly—by linking data about respondents with external information that directly identifies them.

Confidential Information is any identifiable information *or information associated with identifiable* information about a person or establishment collected under an assurance that restricts the degree to which the information can be shared with others.

It is important to understand that information that by itself would not lead to the identity of a respondent, but which could do so if combined with information already released (e.g., the identities of areas in which a survey was conducted), must also be considered confidential.

A *disclosure* occurs when identifiable information concerning an NCHS respondent (including the fact of his participation in an NCHS survey) is made known to a third party. Disclosures may be *authorized* (as when a respondent has consented to the information being so divulged), *unauthorized* (as when information is intentionally revealed to a party not consented to by the respondent), or *inadvertent* (as when a tabulation or file is unintentionally made available to

the public that reveals or can be used to reveal personal information provided by an NCHS respondent). Authorized disclosures are discussed in Section 8, while the prevention of inadvertent disclosure is treated in Sections 9 and 10.

An *agent* is a person designated by an agency to perform, either in the capacity of a Federal employee or otherwise, activities authorized by law and specified in a written document under the supervision or control of an officer or employee of that agency, and who has agreed in writing to comply with all provisions of law that affect the activities conducted on behalf of the agency.

A *collaborator* or collaborating party is one with whom NCHS has a formal working relationship at the inception of a survey or project. In most circumstances, a formal working arrangement is defined in such documents as a Memorandum of Understanding (MOU) or Interagency Agreement (IA), but may also be defined in other appropriate instruments. Although the nature of the working relationship may vary from collaborator to collaborator, the description of that relationship must be very specifically stated in whichever instrument is chosen. A collaborator must have established a formal working arrangement with NCHS at the initial planning and design stages. Thereafter, the collaborator must have tangible and significant involvement in the planning, design, funding, or execution of the survey or project. A collaborator can be, but is not limited to, other Federal agencies, State governments, universities, organizations, colleagues, and others working outside NCHS.

Consent is written, oral, or inferred approval by an NCHS respondent to provide the requested information. Before eliciting information, respondents are clearly informed about the uses to be made of data he or she is asked to supply and the parties who would receive it in identifiable form. This information must be provided in such a way as to represent a full exposure of the facts the respondent needs to make an intelligent decision concerning the provision of personal information to NCHS.

4. Employee Responsibilities

4.1 Division and Office Directors

Each division and office director in the Center has responsibility for assuring staff compliance with NCHS policies pertaining to the confidentiality of records in cases where an assurance of confidentiality has been or is to be given.

4.2 Confidentiality Officer

The Confidentiality Officer will be available to assist the Center Director and staff in a variety of ways, including:

a. Interpreting Department policies pertaining to confidentiality;
b. Assisting employees in obtaining information on and clarification of confidentiality law and related regulations;
c. Directing the NCHS Disclosure Review Board (see Section 9.2) in the review of electronic data products proposed for public release;
d. Providing orientation for new employees, ongoing training for current employees, and implementing appropriate exit procedures to departing staff;
e. Reviewing data collection instruments and procedures;
f. Providing guidance in the development of appropriate inter- and intra-agency agreements, and contractual language for the sharing and collection of confidential information;
g. Conducting periodic physical inspections of NCHS offices to assure that requirements for the physical security of confidential records are observed (See Section 7); and
h. Providing advice regarding appropriate disciplinary action that may be taken when laws, rules, or regulations relating to confidentiality are violated.

4.3 Supervisors' Responsibilities

The Supervisors' Responsibilities include the following:

a. Supervisors will inform all employees, and subsequently all new employees, of existing NCHS policies and procedures relating to the subject of confidentiality and will discuss with such employees their responsibilities in this area.
b. Supervisors will be responsible for assuring that all employees under their jurisdiction comply with regulations applying to the disclosure of official information that permits the identification of individuals or establishments.

c. Supervisors should recognize unique situations that call for more than usual precautionary measures and should make recommendations for improvement, if necessary.

4.4 Individual Federal Employee's Responsibilities

a. Individual employees are expected at all times to follow the principles and obey the laws, rules, and regulations that are cited or referenced in this manual. When in doubt, employees should obtain advice from the supervisor or the Confidentiality Officer.
b. Each employee of NCHS is responsible for maintaining and protecting at all times the confidential records, in whatever form or media, which are in the employee's presence or under the employee's control.
c. To assure that the employee is fully aware of his responsibilities, each person, on entering employment in NCHS, is given the Nondisclosure Affidavit found in Appendix B to read and sign. They are asked to reasign this form annually.

4.5 Contractors' and Agents' Responsibilities

Persons working under contract to or who are otherwise considered agents of NCHS are subject to the same laws and regulations as NCHS employees. In accordance with the confidentiality provisions incorporated in all NCHS contracts, contractors and agents, and contractor employees are expected to observe all Departmental and Centers for Disease Control and Prevention (CDC) rules and regulations and NCHS policy relating to official information for which confidentiality assurances have been given.

When in doubt concerning any confidentiality law, regulation or practice, advice should be obtained from the NCHS project officer or the NCHS Confidentiality Officer.

Each agent and contract employee of NCHS is responsible for maintaining and protecting at all times the confidential records, in whatever forms or media, that are in their presence or under their control. In addition, they must at all times follow the principles and obey the laws, rules, and regulations that are cited or referenced in this manual. To assure that the agent or contractor employee is fully aware of his responsibilities, each person, on entering on duty, signs a Nondisclosure Affidavit (Appendix C), which spells out the particulars of the laws covering their conduct while under contract to NCHS.

4.6 Collaborator's Responsibilities

Although consent will have been obtained from respondents for access to confidential data by collaborators (See definition of collaborator in Section 3 above), it is nonetheless NCHS policy that sharing of confidential data outside the Center requires positive assurances that they will be accorded the same rigorous care as they receive within NCHS. Accordingly, collaborators are not permitted to receive confidential data unless they have provided such assurances and, in doing so, committed themselves to following the principles and obeying the laws, rules, and regulations cited in this manual. Appropriate model agreements are available for this purpose.

4.7 Administrative Officer's Responsibilities

Each new employee or contractor is required to view a confidentiality video, sign a confidentiality pledge, and receive documents and material dealing with their responsibilities with respect to confidential information while working at NCHS. The Administrative Officer is responsible for making sure that persons entering on duty at the Center comply with all appropriate requirements established by the Confidentiality Officer. Similarly, upon departure from NCHS employment, staff are required to undergo a well-defined exit process. The Administrative Officer is responsible for ensuring that departing staff comply with all requirements.

5. NCHS Policies on Consent and Assurances of Confidentiality

5.1 Consent

Obtaining consent from individuals. Consent may be obtained by means of a signature or by construction. In the first instance, the respondent may be provided a written description of the intended treatment of information he/she is asked to

provide and asked to sign his/her name, thereby indicating permission to use that information as described. In some cases, however, he/she is given this information either in writing or verbally. If the respondent then supplies the requested data, NCHS ''construes'' that the respondent agrees to those intended uses and sharing of data with parties he has read or been told about. The Center can then make such uses of the data as have been described to the respondent, but no other uses of the data may be made. In arriving at the content of a statement of consent, the Confidentiality Officer and the Chair of the NCHS Research Ethics Review Board (ERB) cooperate closely. All protocols submitted to the ERB are reviewed for conformance with NCHS confidentiality requirements, and the final, consent documents must be placed on file with the Confidentiality Officer prior to use in the field. (NOTE: Following confidentiality requirements does not release staff from the requirements of the ERB.

Obtaining consent from an establishment. In the case of establishments, the approach depends partly upon whether the request for information is made in a personal interview or by mail.

A. If the request for information is made in person by a staff member or agent of NCHS, the contact person first inquires as to who is authorized to provide the requested data on behalf of the establishment. When such authorized person is informed of the uses to be made of the data, and he/she then supplies the data, NCHS staff construes that the establishment has given consent to the uses of data as specified.
B. When data are sought from an establishment by mail, the request may be addressed to the establishment itself, to the manager of the establishment, or to some other person who, as the Center has previously ascertained, is authorized to provide requested data on behalf of the establishment. The letter transmitting the request explains the uses to be made of the data. When NCHS staff then receives the requested data from the establishment, it is construed that the establishment has consented to those uses of which it has been informed.

5.2 Assurances of Confidentiality

Background. Whenever NCHS requests data concerning an individual or an establishment, it is obligated to provide certain information and assurances to the supplier of information. Although this is considered a moral obligation by NCHS, it is also stated or implied in both the Public Health Service Act and the Privacy Act of 1974. The Public Health Service Act, in Section 308(d) states that information may not ''be used for any purpose other than the purpose for which it was supplied;'' therefore, such purposes must be explained to the supplier of information before obtaining the information from him/her. The Privacy Act of 1974 states in Section (e)(3) that the agency shall:

> Inform each individual whom it asks to supply information, on the form that it uses to collect the information or on a separate form that can be retained by the individual. . .
>
> A. the authority (whether granted by statute, or by executive order of the President) which authorizes the solicitation of the information and whether disclosure of such information is mandatory or voluntary;
> B. the principal purpose or purposes for which the information is intended to be used;
> C. intended disclosure (if any) of identifiable information to other parties; and
> D. the effects on him/her, if any, of not providing all or any part of the requested information.

Such information must be consistent with the information in the description of the system of records published in the Federal Register. *If any release of any identifiable information is to be made, then the law requires that consent be obtained in advance for that specific release*. The Public Health Service Act, Section 308(d) states that ''such information may not be published or released in other form if the particular establishment or person supplying the information or described in it is identifiable unless such establishment or person has consented (as determined under regulations of the Secretary) to its publication or release in other form.'' The Privacy Act (in 552A(b) states that, with certain exceptions, an individual's record may not be disclosed except pursuant to a written request by, or ''with the prior written consent of the individual to whom the record pertains.''

Statement of assurances. The set of information given to any individual or establishment asked to provide data to the Center must include a statement of assurances. This must include:

(1) The legal authorization(s) for soliciting the data (in the case of NCHS, the Public Health Service Act);
(2) The purposes for which the data are being collected and the parties with whom identifiable information will be shared;
(3) The voluntary nature of the response;
(4) The consequences, if any, to the respondent for failing to provide any part of the requested data; and

(5) An assurance that the Center will protect the data against other uses.

5The statement of assurances may be contained in a letter or brochure handed or mailed to a respondent so that he/she receives it before providing the information. The statement may be given orally to a respondent, but it also must be provided in written form, on paper, to be retained by the respondent; the only exceptions to this requirement are: (a) if a self-administered questionnaire is used, the statement may be made part of the questionnaire, and no separate copy need be given to the respondent, and (b) in the case of a telephone interview, an oral reading may be sufficient (see ''Section 5.6'').

The assurance of confidentiality constitutes the guarantee given to the data supplier that NCHS will limit its uses of the data to those specified to the respondent and that NCHS will actively protect the information from any other uses by any other party.

5.3 Responsibility for Formal Assurances of Confidentiality

Formal assurances of confidentiality will be given by the Director of NCHS or his designee. Such authority is vested in the Director of the Center and the Director of each of its divisions and offices. However, incidental references to the assurances are permitted in communications signed by other staff members such as survey managers directly involved with the development and negotiation of such assurances. In view of the complexities involved in confidentiality assurances resulting from legislative and regulatory requirements, Division and Office Directors are required to submit the confidentiality assurances relating to each data collection program to the Confidentiality Officer for review and approval. This approval should be obtained before the Request for Clearance goes to the NCHS Research Ethics Review Board or OMB Clearance Officer.

5.4 Data Collected Directly From Individuals or Establishments

Whenever data are to be collected with a promise of confidentiality[2] directly from individuals or establishments by an employee, agent, or contractor of NCHS, primarily to accomplish an NCHS function, the following rules governing assurances and information are to be met:

1. Include on the data collection instrument (whether electronic or paper) in a clearly visible location and in clearly visible letters the following notice (or words to this effect) of the confidential treatment to be accorded the information in the instrument by anyone who may see it:

Confidential Information

''Information contained on this form which would permit identification of any individual or establishment has been collected with a guarantee that it will be held in strict confidence, will be used only for purposes stated in this study, and will not be disclosed or released without the consent of the individual or the establishment in accordance with Section 308(d) of the Public Health Service Act (42 U.S.C. 242m) and the Confidential Information Protection and Statistical Efficiency Act.''

2. On a letter or other form that can be retained by the individual or the establishment, or on the questionnaire form itself if it is a self-administered questionnaire, inform in clear and simple terms each individual or establishment asked to supply information:
   a. That the collection of the information is authorized by Section 306 of the Public Health Service Act (42 U.S.C. 242k);
   b. Of the purpose or purposes for which the information is to be used, clearly stating that the records will be used solely for statistical research and reporting purposes;
   c. Of intended disclosures (if any) of identifiable information to other parties;
   d. That participation is voluntary and there are no penalties for declining to participate in whole or in part; and
   e. That information will not be used for any purpose other than statistical research and reporting, nor will it be shared in identifiable form with anyone other than named agencies and collaborators.

[2]In the rare instance in which data are collected without a promise of confidentiality, permission to collect the data must be granted by the Director, NCHS.

When social security number or Medicare claim number (which may incorporate the social security number) are collected, respondents must, at the point of collection of that information, be informed, in clear and understandable language of items a through d.

5.5 Data Collected From Another Organization

Whenever the Center arranges to purchase or otherwise obtain from another organization data that contain identifiers of individuals or establishments, it will provide to the supplier the information specified in the previous items 5.4 2a, b, c, and e. This information will be provided in written form, either in the contract, purchase order, or other written statement.

5.6 Data Collected Over the Telephone

Whenever data are to be collected *over the telephone* by an employee, agent, or contractor of NCHS, primarily to accomplish an NCHS function, the following rules governing assurances and information are to be met:

1. Before eliciting survey information from a respondent in any telephone survey, the respondent will be given the following information (though not necessarily with this exact wording) over the telephone:

   a. The law authorizing collection of the information. If the survey is being conducted under the Center's legal authority, the interviewer should say, ''The survey is being conducted under authority of the Public Health Service Act.'' If the respondent requests the specific legal citation, the interviewer will say that it is Volume 42 of the U.S. Code, Section 242k.
   b. The purpose or purposes for which the information is to be used, such as ''for statistical research on health problems.''
   c. That participation in the survey is purely voluntary.
   d. Any possible disclosures of identifiable data to be made outside NCHS.
   e. An assurance that (except for any such disclosures) the confidentiality of all information supplied will be carefully protected, and no one other than NCHS and its agents and any collaborators will have access to any data that identify the respondents.

The exact wording proposed for informing respondents in any particular survey may vary from that suggested above, but must be submitted for approval by the Confidentiality Officer prior to the request for OMB approval.

2. The telephone interviewer must sign a statement that the information required (as indicated above) was given orally to each respondent. This information shall be given by reading the approved text and answering any of the respondent's questions about it before proceeding with the interview. The statement to be signed by each interviewer may be on the form used to collect the survey data.

   In computer-assisted telephone interviewing where there is no hard copy questionnaire, the following procedure may be used in lieu of having the interviewer sign a statement: Following the prompting for the interviewer to read the prescribed statements to the respondent, the computer then asks the interviewer whether he or she certifies that he/she has read to the respondent all the statements, in their entirety, contained in items _____ through _____. *If so*, the interviewer is asked to touch Y (or another appropriate symbol) for "*yes,*" and to enter his/her personal identifier code and the date. The computer then checks whether these have been entered correctly and, if they have, the computer makes this certification a permanent part of the interview record. If they are not entered correctly, the computer will not proceed with the interview.

5.7 Repository of Assurances

A. A central repository for the filing of statements of assurances has been established under the supervision of the Confidentiality Officer.
B. Each organizational unit of NCHS, which has given statements of assurances, will forward copies of all such statements to the repository. This will normally include but, not be limited to, assurances given in contracts, special letters, brochures, survey questionnaires, and forms.
C. The assurances submitted to the Confidentiality Officer for approval will be filed in the Repository of Assurances

as a tentative issuance. When all clearances have been received and final printed copies of the survey or study materials have been produced, a copy of these materials is forwarded to the Repository to replace the tentative materials.

6. Treatment of Requests for Information Under the Freedom of Information Act

Whenever a request is received for a specified record[3] concerning a named individual, that request is subject to requirements of the Freedom of Information Act (FOIA). With certain exceptions, this law requires that Federal agencies provide copies of requested records. There are, however, two important exceptions to the requirement that usually apply to the Center. They are (1) ''personal and medical files and similar files, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy'' and (2) matters specifically exempted from disclosure by statute. In the case of NCHS, Section 308(d) of the Public Health Service Act specifically exempts personal information from disclosure. Requests to NCHS for records under FOIA, where there is a named individual, are not subject to FOIA when data are identifiable.

Policy. If an employee receives a request for a record or an item of information that cites the FOIA, he should immediately refer this request to the NCHS Freedom of Information Act Coordinator as response must be made within 10 days. Any request for information where there is any doubt as to whether it can be provided shall be referred to the Confidentiality Officer.

7. The Protection of Records and Data Systems

Employees of NCHS are responsible for protecting all confidential records from prying eyes, unauthorized access, theft, and from accidental loss or misplacement due to carelessness.

On this subject the Privacy Act, in Section 552a(e) prescribes that each agency shall:

(9) Establish rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records, or in maintaining any record, and instruct each such person with respect to such rules and the requirements of this section, including any other rules and procedures adopted pursuant to this section and the penalties for noncompliance;

(10) Establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained. . . .

In the case of NCHS, the *Staff Manual on Confidentiality*, taken as a whole, together with other administrative practices, fully addresses these requirements. Particular attention is directed to two major aspects: the protection of confidential records and the security of automated data systems.

7.1 Physical Protection of Confidential Records

Absolute protection of the records would be impossible; nevertheless, all reasonable precautions must be taken to protect them.

It is the policy of NCHS that:

A. Confidential records must be kept locked up at all times when they are not being used. That is, they must be kept in locked cabinets or in locked rooms after business hours and whenever the persons using them are not present. If records are maintained in electronic form, the medium on which the files are stored (floppy disks, CD-ROMS, and removable hard drives) must also be kept in locked containers or, if maintained on a computer, access secured by all available means (including keyboard locks, passwords, encryption, office locks, etc.). Personal computers

[3]''Record'' is defined in the Department's regulations (45 CFR Part 5) as including ''books, brochures, punch cards, magnetic files, paper tapes, sound recordings, maps, pamphlets, photographs, slides, motion pictures, or other documentary materials. . .'' In the case of NCHS, other examples of a ''record'' would be videos, x rays, and tissue or blood samples as well as electronic files in whatever form—CD-ROMS, diskettes, etc.

containing confidential records should never be maintained in an open, unsecured space. Only a limited number of staff, as authorized by the Division or Branch Chief, may have keys or other means of access to such cabinets or rooms.

B. When confidential records are in use, whether by themselves or viewed on computer monitors, they must be kept out of the sight of persons not authorized to work with the records.

C. Except as needed for operational purposes, copies of confidential records (paper documents, electronic files, video recordings, or records of other kinds) are not to be made. Any duplicate copies made of confidential records are to be destroyed as soon as operational requirements permit. Records not otherwise covered by record retention regulations (when in doubt, consult the NCHS Records Management Liaison) that are no longer needed should also be destroyed. Approved means of destruction include shredding, burning, and macerating. Should reuse of electronic media (hard drives, rewriteable compact disks) containing confidential records be contemplated, extreme care should be taken not to dispose of information in such a way that it can be recovered by unauthorized users of the electronic medium involved. For further guidance for the disposition of paper and other types of records, consult the NCHS Information Systems Security Officer.

D. Paper or electronic records containing personally identifying information such as respondent name, address, or social security number should be held to the minimum number deemed essential to perform the Center's functions, kept in a highly secure manner, and kept only so long as needed to carry out those functions. A written justification for maintaining files with these items must be submitted to the Confidentiality Officer and, if approved, access restricted to the smallest number of staff consistent with that justification. The justification must include a statement specifying the time period after which these items will no longer be needed and provision for their subsequent deletion or destruction.

E. No record containing direct personal identifiers (name, address, social security or other identifying number, unretouched video, or audio recording) of NCHS survey respondents may be electronically sent to or accessed from an employee's or contractor's alternate work site or removed from NCHS offices except as required in the conduct of data collection activities. Work outside the Center (whether at home or at an alternative work site) with ''in-house'' files (records stripped of direct identifiers but not approved for public use) must receive approval in advance. Such applications include *all* cases where confidential data would be accessed from outside NCHS offices *and are not limited to flexiplace requests*. The staff member will agree in writing not to download the contents of confidential files accessed from home or from an alternate work site. Confidential files are not approved to be used on laptop computers. Other security requirements as dictated by the NCHS Information Systems Security Officer must also be met.

F. When records are transferred to the National Archives and Records Administration or its record centers for storage, their containers must be sealed. The storage center must be advised that no one may have access to those records except as authorized over the signature of an appropriate official of NCHS. Where destruction of records at a future date is cited in the NCHS Records Schedule, such destruction of records containing personally identifying information must be personally witnessed by the NCHS Records Management Liaison or his/her designee.

G. When records containing names or other direct identifiers are transmitted between NCHS offices or between NCHS and its contractors, they must be packaged securely and sent by the most secure and trackable means available (e.g., Fed Ex, personal messenger, or directly by NCHS staff).

H. Confidential records may not be released outside NCHS (to another agency, contractor, or other party) unless that release is consistent with the assurance of confidentiality under which they were gathered and positive evidence (appropriate contract language, a memorandum of understanding, or interagency agreement) that the receiving party will provide the same level of confidentiality protection as that required of NCHS. Agency staff and any contractors must be made liable to legal sanctions if the confidentiality pledge should be violated, and records must be maintained by the Program or Division under whose direction the information was collected listing all files released (to whom and under what agreement) containing confidential information. Such records should cover files made available to other divisions within NCHS as well as outside the Center.

7.2 Automated Data Processing Systems Security General

In achieving the goals of the Privacy Act of 1974, policy and guidance documents have pointed to the important area of automatic data processing (ADP) in establishing safeguards to ensure the security and integrity of records. Identifiable NCHS data are considered highly sensitive. The DHHS Automated Information Systems Security Program Manual is a Departmental directive which provides practices and procedures intended to carry out OMB Circular A-130, regulates the security of Federal automated information resources. Appendix 3 of the Circular defines ''adequate security''

as ''security commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information.'' All technical, personnel, administrative, environmental, and telecommunications safeguards necessary to protect the ''confidentiality, integrity, and availability'' of NCHS data must be in place. OMB Circular No. A-123, ''Management Accountability and Control'' and the Federal Managers' Financial Integrity Act (FMFIA), also are applicable. The FMFIA carries both fine and imprisonment penalties for misuse of Government resources. These laws are applicable to data collected by NCHS under 308(d). NCHS staff, prior to development of contracts or projects, must consult with the Information Systems Security Officer to ensure compliance with applicable laws and regulations.

Although the System Manager is the Federal official who is legally responsible for the system of records subject to the Privacy Act, all others who control, handle, or use the data also share responsibility for the security and integrity of the records. These include the NCHS Top Secret Coordinator and program Top Secret Administrators, ADP Systems Security Officer, systems analysts, programmers, data preparation personnel, and ADP systems users. Contractors who deal with data that come under the provisions of the Public Health Service Act and/or the Privacy Act are subject to the same regulations as are DHHS employees.

Document Control. While not in use, all documentation containing or relating to identifiable information must be stored in such a manner as to prevent disclosure. This includes:

A. Documentation of functional and program specifications;
B. Documentation illustrating record layouts of files containing personal data;
C. Documentation containing descriptions of internal controls and audit techniques employed within the system;
D. Any other hard copy associated with confidential information;
E. Computer program listings and source decks;
F. Documentation production run procedures; and
G. Documentation related to statistical disclosure limitation procedures and disclosure review.

All ADP systems users should familiarize themselves with the contents of the DHHS Automated Information Systems Security Manual. Center personnel are required to comply with the regulations in this manual.

8. Authorized Disclosures

Governing Principles. NCHS action is governed or constrained by four principles:

A. The action leading to disclosure must be clearly within the relevant laws and regulations, and if there is any doubt, the advice of legal counsel should be sought.
B. The Center must always be *candid* with respondents, making it clear who will have access to individual responses and for what (general) purpose the data are being collected.
C. An essential requirement for release of data is the *consent* of the respondent.
D. The release of confidential data must be carried out under agreement as described in Section 8.3.

8.1 Disclosure to the Parent Locator Service

With but one exception, no information about a person or establishment may be disclosed to anyone without the informed consent of the person or establishment supplying the information or described in it.

That single exception is contained in the 1974 Amendments to the Social Security Act relating to the Parent Locator Service (42 U.S.C. 653) which reads in part:

(b) Upon request, filed in accordance with Subsection (d), of any authorized person (as defined in Subsection (c)) for the most recent address and place of employment of any absent parent, the Secretary shall, *notwithstanding any other provision of law,* provide through the Parent Locator Service such information to such person, if such information-(l) is contained in any files or records maintained by the Secretary or by the Department of Health, Education, and Welfare. . . .

It seems unlikely that any information in the files of NCHS would ever be useful to the Parent Locator Service in locating absent parents. However, if any such request were ever received, it should be referred immediately to the Confidentiality Officer, who will decide the action to be taken.

8.2 Disclosures Permitted by Section 308(d) of the Public Health Service Act

Under Section 308(d), NCHS is permitted to publicly release data for identifiable individual persons or establishments if (1) such release is included in the purpose for which the data were supplied, and (2) the particular person or establishment supplying the information or described in it has consented to such release. This is an extremely rare occurrence. The only two instances have been the release of establishment names in directories of facilities included in the Master Facility Inventory and the playing of NCHS Questionnaire Design Research Laboratory videotapes showing respondent's faces at professional meetings. In both cases, great care was taken to obtain informed consent from respondents.

If the information to be released relates to one or more identified individuals, then the requirements for disclosures contained in the Privacy Act of 1974 (see, for example, § 552b of the Act would also have to be met. Such disclosures would, nevertheless, be a departure from common Center practices on confidentiality.

8.3 Disclosures Within NCHS

Although consent for the use of confidential data does not restrict their use to the program that collected them, programs are, nonetheless, responsible for their use by other programs within the Center. Therefore, division-level approval is required for the use of confidential data by other NCHS programs. This will involve the preparation of a transmittal memorandum specifying the NCHS staff member to be granted access and the purpose and anticipated duration of use of the data. The memorandum should mention that the receiving division may not pass the file on to others without the approval of the originating division. These memos should be kept on file in division offices.

8.4 Disclosures Within the Department

The Privacy Act of 1974 considers DHHS in its entirety as one agency, and it permits the disclosure of records ''to those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties.'' (Section 552a(b)(l)). The Public Health Service Act also permits identified data in NCHS to be transferred to other parties provided that consent has been obtained for such transfer prior to the record's being supplied to NCHS. It must be stressed, however, that these laws do not *require* NCHS to disclose confidential records to other parties. If there is any other way in which a data requestor's needs can be met, that alternative should be given precedence. In any event, *NCHS would not transfer any confidential data to another part of the Department without positive assurance that the data will be used only for the authorized purpose, and that the confidentiality of the data will be protected quite as effectively in the other organization as it would be by NCHS itself. NCHS reserves the right not to transfer confidential data to anyone if it is not convinced that those data will be handled appropriately*.

Such assurance should take the form of an Interagency Agreement, Memorandum of Understanding, or other formal agreement providing details concerning applicable law and government regulation, permissible disclosure, legal responsibilities, treatment and disposition of confidential records, and the designation of specific persons responsible for the security of such records. Whatever their form, any document developed for the transfer of confidential records from NCHS to another agency must clearly document that consent for such a transfer was obtained from respondents, have the written approval of the *Director of NCHS* and be signed by the Director of the Agency receiving the records or other person with sufficient legal and administrative responsibility to commit the agency or executive.

8.5 Transfers of Data to Other Departments of the Federal Government

Section 3510 of the Paperwork Reduction Act of 1980 provides:

(a) The Director (of the Office of Management and Budget) may direct an agency to make available to another agency, or an agency may make available to another agency, information obtained pursuant to an information collection request if the disclosure is not inconsistent with any applicable law.

Aside from interdepartmental disclosures between the Center and the U.S. Census Bureau, involving the surveys that the U.S. Census Bureau conducts on behalf of the Center, transfers are rarely made to other departments. Although such exchanges may take place, they are not to be undertaken unless they conform to the Privacy Act of 1974, the Public Health Service Act, and any other relevant Federal laws. In particular, respondents must have been clearly and fully informed of the Center's intent to share information with an agency outside DHHS, the extent of the information shared, and the purpose for which the information will be released. As with other releases of information outside NCHS, the

interdepartmental transfer of data may be done only with the express approval of the Director of NCHS under an agreement as described in Section 8.4. In addition, *NCHS would not transfer any confidential data to another department without positive assurance that the data will be used only for the authorized purpose and that the confidentiality of the data will be protected quite as effectively in the other organization as it would be by NCHS. NCHS reserves the right not to transfer confidential data to anyone if it is not convinced that those data will be handled appropriately*.

8.6 Special Cooperative or Contractual Arrangements

NCHS may be a party to any of several types of arrangements in which the Center is but one of two or more organizations that are collecting, processing, or using data under a joint or cooperative agreement. These types of situations are not discussed in detail in this manual, but three prominent classes of cases are identified:

A. A special situation prevails in the Vital Statistics Cooperative Program, where the State is the collector under its own law. The Center uses the data under a contractual arrangement with the State, which fills the role of respondent in this context. The Center abides by the terms of the contracts, although it can exercise no control over how the State manages other confidentiality aspects of its documents. Under the terms of the State contracts, NCHS will not permit access to individual documents that may be in its possession for coding purposes; nor will NCHS give the ''key'' (certificate number) to individual certificates to anyone without the express written consent of the State (registration area). Under special arrangements, NCHS makes available to the public microdata files containing person-record information.
B. Contractual arrangements exist in which another person or organization either (1) provides a service—such as field collection—to NCHS, or (2) undertakes analysis of data provided by NCHS and, in either case, has access and de facto control of microdata. (See ''Appendix A'' for confidentiality requirements in such contracts.)
C. Other instruments that legally obligate other parties to NCHS nondisclosure rules and obligations include professional service contracts, task orders, intergovernmental personnel act (IPA) appointments, unfunded memoranda of agreement, interagency, and intra-agency confidentiality agreements. If not already included, the language contained in Appendix A must be made part of all such documents.

Certification (NCHS Confidentiality Pledge) must be included within these documents indicating that the party or parties receiving identifiable NCHS data understand their obligation to abide by all NCHS rules and regulations. Specific wording for each document of this type should be developed in consultation with the NCHS Confidentiality Officer who must, along with the NCHS Director, approve the final wording.

9. Avoiding Inadvertent Disclosures Through Release of Microdata

It is Center policy to make its files on individual elementary data units widely available to the scientific community so that additional analyses can be made of these data for the country's benefit. The scientific community has shown great interest in such files, and many requests for the Center's electronic files are received each year.

9.1 Problem

A microdata file consists of individual records each containing values of variables for a single person or establishment. Even when all personal identifiers are removed, a large amount of information remains, and this information may identify NCHS respondents to a person who has access to that information from another source. For example, if file descriptors indicate that the respondent is a Ph.D. in the 30–34 years age group who reports his/her race as white and lives in the Northeast section of the country, the respondent is not identifiable. If, however, the file indicates that his age is 31, that he is married to a 42-year-old woman who reports her race as Asian, has three children, and lives in Litchfield County, Conn., the respondent may now be identified uniquely, and all information in the file about him and his family would be disclosed to anyone with access to the file (who could then identify the person from the given set of characteristics or by matching this information to that contained in another file containing the respondent's name). The place of residence, especially when it is not a heavily populated area, is particularly useful in the identification process. Moreover, if it is known that a particular person or establishment has been selected in the sample, chances are much better that the person or establishment can be identified. In such cases, information may be known to a potential intruder who can be used to establish identity.

It should be recognized that the information gained by an intruder need not be *exact* to represent a disclosure if it pertains to an identified individual. Tables (see ‘‘Section 10’’), generated using microdata files, should take into account that it may be possible to associate ranges of values of certain variables (e.g., income, age) with other information. This is particularly applicable to files containing establishment data. In addition, it may be possible to use certain other information contained in the microdata file to identify an individual or establishment. A more detailed discussion of these points is found in Section 10.1.

The low-ratio sample that the Center uses in its surveys would usually frustrate a person who is trying to locate a known individual in the Center’s survey files. From time to time, however, an individual or establishment may have characteristics rarely encountered in the population from which a sample is drawn.

The only absolutely sure way to avoid disclosure through microdata files is to refrain completely from releasing any microdata files, but this would deprive the Nation of a great deal of very important health research. It is the Center’s policy to release microdata files for purposes of statistical research only when the risk of disclosure is judged to be extremely low. In order to make such judgments, the Center has established a Disclosure Review Board (DRB) which meets regularly to consider proposals for public release of microdata files and makes recommendations to the Confidentiality Officer.

All microdata files intended for public release must be submitted for review by the NCHS DRB.

9.2 Rules

The following rules apply to all files released by NCHS that contain any information about individual persons or establishments, except where the supplier of information was told, prior to his giving the information, that the information would be made public:

A. Before any new or revised microdata files are published, they, together with their full documentation, must be approved for publication by the Confidentiality Officer who will rely upon assistance from the NCHS Disclosure Review Board in reaching decisions.

B. The file must not contain any detailed information about the subject that could facilitate identification and that is not essential for research purposes (e.g., exact date of the subject’s birth, excessive detail for occupation, extreme values of income and age, detailed race or ethnicity for small and highly visible groups, and other characteristics that would make an individual or establishment easier to identify). It is recommended that the following be consulted concerning possible techniques that would permit the maximum amount of information to be released consistent with sound principles of statistical disclosure limitation: The Confidentiality and Data Access Committee’s *Checklist on Disclosure Potential of Data* and *Statistical Policy Working Paper 22, Report on Statistical Disclosure Limitation Methodology*. Office of Information and Regulatory Affairs, Office of Management and Budget.

C. Geographic places that have fewer than 100,000 people are not to be identified on the file. Depending upon the statistical structure of a file and other circumstances, a higher figure may be employed. It is the responsibility of the program proposing the data release to determine the disclosure risk associated with the proposed minimum size of geographic areas to be identified.

D. Characteristics of an area are not to appear on the file if they would uniquely identify an area of less than 100,000 people (e.g., a variable describing the size of a metropolitan area in which a respondent was interviewed providing for a category of less than 100,000 in a file where a region is also provided).

E. Information on the drawing of the sample that might assist in identifying a respondent must not be released outside the Center. Thus, *the identities of primary sampling units (PSUs) are not to be made available outside the Center* except in limited circumstances and as approved by the Confidentiality Officer. When such circumstances require the disclosure of the identity of areas in which data collection activities take place, the survey manager must ensure that all information for this survey proposed for release take into account the greater risk of identification because of this exception. The decision as to whether PSU identities are to be made public should be made before data are collected and plans for data release finalized.

This section has described procedures for disclosure review and protection of microdata files. Any tabulations or statistical measures based upon files so prepared and approved for public release by the NCHS Confidentiality Officer would meet NCHS requirements for disclosure protection and, along with the microdata, can be released to the public. In other cases, where tabulations are based upon data in a form not approved for public use, procedures in the following section must be followed.

9.3 Restricted Access to Microdata Files With Identifiable Data

Under certain circumstances, access to microdata files containing high levels of detail such as described in 9.2 B, C, or D, may be granted to researchers in the NCHS Research Data Center (RDC) or by means of the NCHS Remote Data Access System. In the RDC, analytical manipulation of elements of confidential files not released to the public is permitted. Files contain no names, addresses, or other direct identifiers. Because the remaining information would require complex manipulation with other information not permitted in or accessible from the RDC in order to re-identify an NCHS respondent, the researcher has, in effect, no access to identifiable information. Nevertheless, no statistical output can be removed from the RDC without being subjected to statistical disclosure analysis by RDC staff, and access to information within the RDC is highly restricted.

Requests for tabulations may also be submitted electronically. No direct access to confidential files is permitted, however, and only those tabulations that have been subject to statistical disclosure analysis are transmitted back to the requestor.

10. Avoiding Inadvertent Disclosures in Published Tabular Data

The previous section considered detailed procedures for disclosure review and protection of microdata files made available for public use. Any tabulations or calculations based upon data so prepared and approved would meet NCHS requirements for disclosure protection and, along with the microdata, can be released to the public. Where a tabulation is based upon data in a form not approved for public use, the following procedures must be followed.

10.1 Types of Disclosure

Center policy recognizes and attempts to deal with several classes of information disclosure:

A. *Exact versus approximate disclosures*. Exact disclosure is the disclosure of a specific characteristic, such as race, sex, or a particular pathological condition. Approximate disclosure is the disclosure that a subject has a characteristic that falls within a certain range of possibilities, such as being between 45 and 55 years of age or having an income between $15,000 and $25,000. An approximate disclosure may in a given situation be considered harmless because of its indefinite nature.

B. *Probability-based versus certainty disclosures*. Data in a table may indicate that members of a given population segment have an 80-percent chance of having a certain characteristic; this would be a probability-based disclosure as opposed to a certainty disclosure of information on given individuals. In a sense, every published table containing data or estimates of descriptors of a specific population group provides probability-based disclosures on members of that group, and only in unusual circumstances could any such disclosure be considered unacceptable. It is possible that a situation could arise in which data intended for publication would reveal that a highly specific group had an extremely high probability of having a given sensitive characteristic; in such a case the probability-based disclosure perhaps should not be published.

C. *Internal versus external disclosures*. Internal disclosures are those that result completely from data published from one particular study. External disclosures occur when outside information is brought to bear upon the study data to create disclosures. This possibility must be recognized in any disclosure analysis.

10.2 Problem

In an effort to make available to the public a full set of information on a given subject, statisticians may—and sometimes do—present so much detail in published tabulations that they accidentally reveal confidential information about particular study subjects. When *complete count data* are being tabulated* this may happen in the following ways:

1. All cases in line y_i of a statistical table fall in the cell in column x_i. We then know that any individual in the population with characteristic y_i also has characteristic x_i.
2. Cell x_iy_i gives the total income of all individuals with characteristics x_i and y_i. If there are only two individuals, *a* and *b*, in the population with that combination of characteristics, then *a*, knowing his/her own income, will be able to determine *b*'s income by simple subtraction, and *b* will also be able to determine *a*'s income.

*As when all cases in a given stratum have been included in a sample or all vital events are tabulated.

In addition, when establishment data are involved:

1. A table gives the total annual receipts for all five nursing homes in county *m*. However, nursing home *a* is much larger than all the rest combined; it accounts, in fact, for three-fourths of all nursing home receipts in the county. Knowing the county total, the manager of nursing home *a* is able to calculate the incomes of the other four homes, at least within some fairly narrow limits.
2. A metropolitan statistical area (MSA) contains two counties, *a* and *b*. Four hospitals are located in county *a* and only one in county *b*. A statistical report is published, giving confidential hospital data totaled for each SMSA. Another report is published with confidential data on hospitals by county, but only for counties with three or more hospitals. Using the two reports, one can subtract the data for county *a* from the SMSA data, deriving the confidential data for the lone hospital in county *b*.

These examples imply the existence of several general types of situations in which statistical disclosure may occur. An additional possibility may be found in a group of three or more tables of subsets of a given population from which disclosures are possible through the solution of simultaneous equations. Center guidelines as set forth in Section 10.3 take into account the several possible disclosure situations.

10.3 Special Guidelines for Avoiding Disclosure

Except where otherwise indicated, the following guidelines apply to all Center publications of statistics:

A. In no table should all cases of any line or column be found in a single cell.
B. In no case should the total figure for a line or column of a cross-tabulation be less than five unweighted cases.
C. In no case should a quantity figure be based upon fewer than five unweighted cases.
D. In no case should a quantity figure be published if one case contributes a disproportionate amount to the total. A minimum percentage figure should be adopted for this purpose and this figure should not be publicly released.
E. In no case should data on an identifiable case, nor any of the kinds of data listed in preceding items A–D, be derivable through subtraction or other calculation from the combination of tables published on a given study.
F. Data published by NCHS should never permit disclosure when used in combination with other known data.

Report writers are to follow these guidelines. It is the responsibility of all branch chiefs to see that these guidelines are followed. In applying them, branch chiefs are not required to consult with the NCHS Confidentiality Officer. However, if a guideline appears unreasonable in a given situation, approval for a special exception should be requested from the NCHS Confidentiality Officer.

A specific exception not requiring special approval applies in the field of vital statistics. It has been a longstanding tradition in the field of vital statistics not to suppress small frequency cells in the tabulation and presentation of data. For example, it has been considered important to know that there were two deaths from rabies in Rio Arriba County, New Mexico, in a given year, or that there were only one infant death and two fetal deaths in Aitkin County, New Mexico. Public release of such tabular data is consented to by data providers and is in the interest of public health. Special procedures for the release of microdata with low levels of geography and/or exact date of a vital event are in place and are described at http://www.cdc.gov/nchs/nvss.htm.

10.4 Evaluating a Disclosure Problem

There may be mitigating circumstances in a given situation that may make it acceptable to publish data that, strictly speaking, could result in ‘‘disclosures.’’ Such circumstances could provide grounds for requesting the ‘‘special exception’’ to the previously noted rules:

A. When data in a study are based upon a small-fraction sample, for example, less than 10 percent of the universe, it might generally be assumed that disclosure will not occur through published tabulations. However, there could be exceptions. So much detail may be presented that an individual unique in the population is identified through the tables or a member of the sample may find himself/herself and others in the data. The usual rules precluding publication of sample estimates that do not have a reasonably small relative sampling error should prevent any disclosures from occurring in tabulations from sample data. This does not absolve the report writer from reviewing tabulations using the principles presented in this section.
B. The existence of errors or imputations in the data brings some small reduction in the likelihood of disclosure through table publication.

C. Incompleteness of reporting, which often occurs even where studies are supposed to include 100 percent of a given group in the population, also reduces the certainty of any disclosure taking place through publication of data.
D. In some instances the danger of disclosure might be mitigated by the fact that the data in question have no sensitivity. They may already have appeared in a published directory, or they may involve entirely obvious characteristics, or they may relate to an earlier time. Since that time, many changes have occurred so that the data have become completely innocuous.

10.5 Measures to Avoid Disclosure

Two methods are customarily used in the Center to prevent disclosures through tabulations:

A. The table is reduced in size when rows or columns are combined into larger categories, eliminating the particular cells that would otherwise produce disclosures.
B. Unacceptable data in cells are suppressed. When this is done, it is necessary also to suppress other cells in the table to prevent determination of the unacceptable cell figure through subtraction. It is usually necessary to suppress four cells in a cross tabulation in order to avoid disclosure through one cell—the offending cell (x_iy_i), another cell in the same row (x_jy_i), another cell in the same column as the offending cell (x_iy_j), and also the cell (x_jy_j) at the intersect of the additional row and column involved in the newly suppressed cells.

It is recommended that the following be consulted concerning possible techniques that would permit the maximum amount of information to be released consistent with sound principles of statistical disclosure limitation: Sections 4 and 5 of the Confidentiality and Data Disclosure Committee, *Checklist on Disclosure Potential of Data* and *Statistical Policy Working Paper 22, Report on Statistical Disclosure Limitation Methodology*, Office of Information and Regulatory Affairs, Office of Management and Budget.

11. Avoiding Disclosure in Other Types of Published Information

Analyses that produce statistics for publication that are not discussed in other parts of this manual should also be reviewed for disclosure risk. For example, disclosure review should be considered whenever the results of regression analyses will be publicly released. This applies particularly to measures based upon unweighted data[4]. In such instances, the same considerations discussed in the Section 10 will apply.

[4]See Reznek, Arnold P. (2003), ‘‘Disclosure Risks in Cross-Section Regression Models,’’ 2003 Proceedings of the American Statistical Association, Government Statistics Section [CD-ROM], Alexandria, VA: American Statistical Association, forthcoming.

Appendix A.

Requirements Relating to Confidentiality and Privacy in Data Collection and Data Processing Contracts[5]

I. *Purpose*. This appendix provides the wording to be used when the National Center for Health Statistics (NCHS) contracts with any organization for the collection or processing of information that identifies individuals and/or establishments. Such contracts must contain stipulations to assure confidentiality and physical security of the information and to assure that the contractor's employees abide by the stipulations.

II. *Background*. The Privacy Act of 1974 (5 U.S.C. 552a) requires the safeguarding of individuals, and Section 308(d) of the Public Health Service Act (42 U.S.C. 242m) requires the safeguarding of both individuals and establishments against invasion of privacy. As a result of the provisions of these acts, contractors who deal with information identifying individuals and/or establishments must stipulate the appropriate safeguards to be taken regarding such information.

III. *Policy*. The following is to be used in data collection and data processing contracts: If the particular circumstances of a given contract imply the need for different wording, the wording may be changed, provided that the new wording is in keeping with the intentions of this manual and provided that approval for the new wording is obtained from the NCHS Confidentiality Officer[6].

Safeguards for Individuals and Establishments Against Invasions of Privacy

In accordance with Subsection (m) of the Privacy Act of 1974 (5 U.S.C 552a) and Section 308(d) of the Public Health Service Act (42 U.S.C 242m), the contractor and employees of the contractor, are required to comply with the applicable provisions of the Privacy Act and to undertake other safeguards for individuals and establishments against invasions of privacy. To provide these safeguards in performance of the contract, the contractor and contractor employees shall be bound by the following confidentiality assurance: ''In accordance with Section 308(d) of the Public Health Service Act (42 U.S.C 242m), the contractor, you as an employee of the contractor, and NCHS, assure all survey respondents that the confidentiality of their responses will be maintained and that no information will be disclosed in a manner in which an individual or establishment is identifiable, unless the individual or establishment has consented to such disclosure.''

The contractor will release no information from the data obtained or used under this contract to any persons except authorized staff of NCHS.

By a specified date, which may be no later than the date of completion of the contract, the contractor will return all study data to NCHS or destroy all such data, as specified by the contract.

To preclude observation of confidential information by persons not employed on the project, the contractor shall maintain all confidential records that identify individuals or establishments or from which individuals or establishments could be identified under lock and key. Specifically:

- Confidential records must be kept locked up at all times when they are not actually being used. That is, they must be kept in locked cabinets or in locked rooms after business hours and whenever the persons using them are not present.
- If records are maintained in electronic form, the medium on which the files are stored (floppy disks, CD-ROMS, and removable hard drives) must also be kept in locked containers or, if maintained on a computer, access secured by all available means (including keyboard locks, passwords, encryption, etc., and office locks).
- Personal computers, desktop or laptop, containing confidential records should never be maintained in an open, unsecured space. Only a limited number of authorized staff may have keys or other means of access to such cabinets or rooms.

[5]Formerly ''NCHS Staff Manual Guide, General Administration No. 3,'' Supplement 4, dated September 8, 1976.

[6]These situations include unusual cases such as: (1) when the data collection is not covered by the Privacy Act; (2) when the data collection is not covered by Section 308(d) of the Public Health Service Act; and (3) when respondents are advised that all information obtained from them will be made public.

- When confidential records are in use, whether by themselves or viewed on computer monitors, they must be kept out of the sight of persons not authorized to work with the records.
- Except as needed for operational purposes, copies of confidential records (paper documents, electronic files, video recordings, or records of other kinds) are not to be made. Any duplicate copies made of confidential records are to be destroyed as soon as operational requirements permit. Approved means of destruction include shredding, burning, and macerating.
- Should reuse of electronic media (hard drives and rewriteable compact disks) containing confidential records be contemplated, extreme care should be taken not to dispose of information in such a way that it can be recovered by unauthorized users of the electronic medium involved. For further guidance on the disposition of paper and other types of records consult the NCHS Information Systems Security Officer.
- Files containing personally identifying information such as respondent name, address, or social security number should be held to the minimum number deemed essential to perform the work under these contract functions, kept in a highly secure manner, and kept only so long as needed to carry out those functions.
- No record containing direct personal identifiers (name, address, social security or other identifying number, unretouched video, or audio recording) of NCHS survey respondents may be electronically sent to or accessed from a contractor employee's home or telecommuting work site or removed from contractor offices except as required in the conduct of data collection activities.

After having read the attached nondisclosure agreement (pledge), each employee of the contractor participating in this project will sign the nondisclosure statement that indicates he/she has carefully read and understands the assurance that pertains to the confidential nature of all records to be handled in regard to this survey. Each contract employee must also view the NCHS Confidentiality Video. As an employee of the contractor, he/she is prohibited by law from disclosing any such confidential information that has been obtained under the terms of this contract to anyone other than authorized staff of NCHS. He/she understands that under the E-Government Act of 2000, any willful and knowing disclosure in any manner to a person or agency not entitled to receive it, shall be guilty of a **class E felony** and **imprisoned for not more than 5 years**, or fined not more than **$250,000**, or both.

The contractor and his professional staff will take steps to ensure that the intent of the statement of understanding is enforced at all times through appropriate qualification standards for all personnel working on this project and through adequate training and periodic follow-up procedures.

Appendix B.
NCHS Nondisclosure Affidavit for Federal Employees

The National Center for Health Statistics collects, compiles, and publishes general purpose vital and health statistics that serve the needs of all segments of the health and health-related professions. The success of the Center's operations depends upon the voluntary cooperation of States, of establishments, and of individuals who provide the information required by Center programs under an assurance that such information will be kept confidential and be used only for statistical purposes.

NCHS operates under the authority and restrictions of **Section 308(d)** of the **Public Health Service Act** that provides in summary that no information obtained in the course of its activities may be used for any purpose other than the purpose for which it was supplied, and that such information may not be published or released in a manner in which the establishment or person supplying the information or described in it is identifiable unless such establishment or person has consented.

Three specific laws excerpted below provide penalties for unauthorized disclosure of confidential information. Their full text is attached:

Section 513 of PL 107–347: ''Whoever, being an officer, employee, or agent of an agency acquiring information for exclusively statistical purposes, having taken and subscribed the oath of office, or having sworn to observe the limitations imposed by Section 512, comes into possession of such information by reason of his or her being an officer, employee, or agent and, knowing that the disclosure of the specific information is prohibited under the provisions of this title, willfully discloses the information in any manner to a person or agency not entitled to receive it, shall be guilty of a class E felony and **imprisoned for not more than 5 years**, or fined not more than **$250,000**, or both.''

18 U.S.C. Section 1905: ''Whoever, being an officer or employee of the United States or any department or agency thereof, . . . publishes, divulges, discloses or makes known in any manner or to any extent not authorized by law any information coming to him in the course of his employment or official duties. . . which information relates to trade secrets, confidential statistical data . . . except as provided by law, shall be **fined** under this title, or **imprisoned** not more than one year, or both; and shall be **removed from office** or employment.''

Privacy Act of 1974, 5 U.S.C. Section 552a(i)(l): ''Any officer or employee of an agency, who by virtue of his employment or official position, has possession of, or access to, agency records which contain individually identifiable information the disclosure of which is prohibited by this section or by rules or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, **shall be guilty of a misdemeanor and fined not more than $5,000**.''

Your signature below indicates that you have carefully read and agreed to follow all NCHS policies and procedures to protect the confidentiality of data collected under these statutes.

Type or Print Name	Date
Signature	NCHS Division/Program (type or print) (Ex: ORM, DHES, DVS, OPBL)
Type of Appt./Length of Appt.	

Appendix C.
NCHS Nondisclosure Affidavit for Contractors

The National Center for Health Statistics collects, compiles, and publishes general purpose vital and health statistics that serve the needs of all segments of the health and health-related professions. The success of the Center's operations depends upon the voluntary cooperation of States, of establishments, and of individuals who provide the information required by Center programs under an assurance that such information will be kept confidential and be used only for statistical purposes.

NCHS operates under the authority and restrictions of **Section 308(d)** of the **Public Health Service Act** that provides in summary that no information obtained in the course of its activities may be used for any purpose other than the purpose for which it was supplied, and that such information may not be published or released in a manner in which the establishment or person supplying the information or described in it is identifiable unless such establishment or person has consented.

The laws excerpted below provide penalties for unauthorized disclosure of confidential information. Their full text is attached:

> **Section 513 of PL 107–347:** ''Whoever, being an officer, employee, or agent of an agency acquiring information for exclusively statistical purposes, having taken and subscribed the oath of office, or having sworn to observe the limitations imposed by Section 512, comes into possession of such information by reason of his or her being an officer, employee, or agent and, knowing that the disclosure of the specific information is prohibited under the provisions of this title, willfully discloses the information in any manner to a person or agency not entitled to receive it, shall be guilty of a **class E felony** and **imprisoned for not more than 5 years**, or fined not more than **$250,000**, or both.''
>
> **Privacy Act of 1974, 5 U.S.C. section 552a(i)(l):** ''Any officer or employee of an agency, who by virtue of his employment or official position, has possession of, or access to, agency records which contain individually identifiable information the disclosure of which is prohibited by this section or by rules or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, **shall be guilty of a misdemeanor and fined not more than $5,000**.''

Your signature below indicates that you have carefully read and agreed to follow all NCHS policies and procedures to protect the confidentiality of data collected under these statutes. You also agree not to link NCHS files with any other file that would permit the identification of an NCHS respondent unless the linkage is conducted under an approved project.

Type or Print Name	Date
Signature	NCHS Division/Program (type or print) (Ex: ORM, DHES, DVS, OPBL)
Contract Company	

Appendix D.
Confidentiality, Security, and Related Contact Persons

Confidentiality Officer	Alvan O. Zarate	(301) 458-4601	AOZ1@cdc.gov
Information Systems Security Officer	John Macias	(301) 458-4370	JMacias@cdc.gov
Freedom of Information Coordinator	Mary I. Jones	(301) 458-4305	MIJones@cdc.gov
Privacy Act Liaison	Mary Moien	(301) 458-4389	MXM3@cdc.gov
Records Management Liaison	Sharon K. Faupel	(301) 458-4201	SFaupel@cdc.gov
OMB Clearance Officer	Mary Moien	(301) 458-4389	MXM3@cdc.gov
Research Ethics Review Board, Chair	Stephen J. Blumberg	(301) 458-4107	SWB5@cdc.gov
Research Ethics Review Board, Vice Chair	Ajani Chandra	(301) 458-4138	AYC@cdc.gov