DEPARTMENT OF HEALTH & HUMAN SERVICES

Public Health Service
Centers for Disease Control and Prevention

National Center for Health Statistics
3311 Toledo Road, Room 7122
Hyattsville, Maryland 20782

MEMORANDUM

Date: **March 26, 2014**

From: Eve Powell-Griner, Ph.D., CIPP/G
Confidentiality Officer
National Center for Health Statistics
Centers for Disease Control and Prevention

Subject: Annual Report from the National Center for Health Statistics to the Office of Management and Budget as required in the Implementation Guidance for Title V of the E-Government Act, Confidential Information Protection and Statistical Efficiency Act of 2002 (CIPSEA) dated June 15, 2007

To: Brian Harris-Kojetin, Ph.D.
Statistical and Science Policy Office
Office of Information and Regulatory Affairs
Office of Management and Budget

The National Center for Health Statistics (NCHS) is filing the annual report as required by the June 15, 2007 CIPSEA Implementation Guidance. This report covers 2013 for the listing of data collections covered by CIPSEA.

Use of the CIPSEA Confidentiality Pledge

Attachment 1 is a listing of the data collections that were covered by CIPSEA and had an active clearance during 2013. In addition, one survey which is OMB clearance-exempt is shown.

The following statement appears on all NCHS data collection instruments:

All information which would permit identification of any individual, a practice, or an establishment will be held confidential, will be used for statistical purposes only by NCHS staff, contractors, and agents only when required and with necessary controls, and will not be disclosed or released to other persons without the consent of the individual or the establishment in accordance with section 308(d) of the Public Health Service Act (42 USC 242m) and the Confidential Information Protection and Statistical Efficiency Act (PL-107-347).

Attachment 2 contains an example of an NCHS survey pledge.

Compliance with the CIPSEA Implementation Guidance

With the assistance of the NCHS Information Systems Security Officer and OMB PRA Clearance Officer, the NCHS Confidentiality Officer reviews NCHS confidentiality and security procedures for adherence to OMB CIPSEA standards as set forth in the June 15, 2007 Implementation Guidance. This review involves all interagency agreements for offsite access to CIPSEA-protected information as well as all proposed data collection approval requests as they move through the PRA OMB clearance process. For data collections that are OMB exempt, the CIPSEA requirements are monitored during the NCHS Ethics Review Board process.

The agency affirms its determination to have the Center be in general compliance with OMB Implementation Guidance. We affirm compliance with the following specific elements or note exceptions or areas the agency is working to come into full compliance:

1. Physical and Information Systems Security: only persons authorized are permitted access to confidential information stored in information systems. NCHS is in compliance through the direction of the NCHS Information Systems Security Officer.

2. Confidentiality Training: all employees are certified annually. Every employee, contractor, fellow, etc. who enters NCHS employment completes the NCHS confidentiality training (see: http://www.cdc.gov/nchs/about/policy/confidentiality_training/index.html), and signs a nondisclosure affidavit documenting CIPSEA and other legislatively-mandated confidentiality requirements. In winter 2013, every person at NCHS completed the NCHS confidentiality training and signed a new nondisclosure affidavit.

3. Record Keeping: the agency has records that identify all individuals accessing confidential information.

4. Review of Information Prior to Dissemination: the agency has in place a process to review information prior to dissemination to ensure that confidential information is not disclosed. The NCHS Disclosure Review Board reviews and approves all electronic data files prior to release. Division/Office staff is responsible for reviewing and approving all tabular data and reports. The Research Data Center staff review output prior to releasing it to researchers working on-site or off-site using ANDRE (remote access system).

Use of Agents Provision in CIPSEA

An example of the full interagency agreement, statements provided by on-site agents and NCHS Research Data Center (RDC) users, and NCHS CIPSEA contract language are provided in Attachments 3-5.

Provision of the number of individual agents NCHS has designated during calendar year 2013 in the following categories:

1. Contractors: NCHS had 88 contract employee agents on-site and 2,593 off-site contractor agents in CY 2013. Approximately 95 percent of contractor agents were involved in data collection related activities.

2. Federal or State Agencies: In CY 2013, NCHS had designated agent agreements with 14 federal agencies/units. There were 2,682 federal agency/unit employee agents, of which 2,548 (95%) were Census staff involved in data collection or management activities on behalf of NCHS. There were no agents from a state agency.

3. Researchers: In CY 2013 NCHS had 391 individual researcher agents. Of these, 118 individuals accessed the information off-site at the researcher's institution and 273 accessed data via NCHS controlled sites (e.g. a research data center).

Provision of information on NCHS compliance with the elements in Section IV of the CIPSEA Implementation Guidance concerning Requirements and Guidelines for Statistical Agencies or Organizational Units When Designating Agents to Acquire or Access Confidential Information Protected under CIPSEA. The agency's report should affirm its compliance with the following specific elements or note any exceptions or areas where the agency is working to come into full compliance:

1. Contracts and Written Agreements: all contracts or agreements include the appropriate provisions in the Appendix of the CIPSEA Implementation Guidance. As a NCHS example, Attachment 5 contains language from a contract for medical coding.

   Physical and Information Systems Security: For research users of NCHS data, NCHS adopted the policy that data released to *another CDC Center* would not require a physical inspection as long as the NCHS Information Systems Security Officer (ISSO) was satisfied that the data would be treated in conformance with CDC security standards and that the requirement that CDC Policy will be adhered to is included in the original agency agreement. The result of this practice is that data held by another CDC Center would be subject to the same security as that at NCHS**.** In agreements with non-CDC Federal agencies, the NCHS ISSO was consulted and submitted to CDC detailed security certification and accreditation statements provided by the agency involved for final vetting by the CDC Chief Information and Privacy Officer. For all other agreements, the NCHS ISSO consulted directly with his counterpart in the other organizations to review security standards and policies.

   NCHS is committed to conducting an inspection of non-federal off-site facilities at least once during the data access agreement period. During 2013, one off-site inspection was conducted.

2. Confidentiality Training: all agents are certified annually. All agreements stipulated the annual recertification of agents.

3. Record Keeping: the agency has records that identify all agents with access to confidential information. For all research agreements, the NCHS Confidentiality Office has records that identify those agents.

Per guideline instructions, this memorandum with attachments will be posted on the NCHS website.

Sincerely,

/Eve Powell-Griner/

Eve Powell-Griner, Ph.D., CIPP/G

cc:
Mr. Rothwell
Dr. Madans
Dr. Buie
Mr. Macias

Attachment 1. NCHS Data Collection Activities conducted under CIPSEA (activities with an active clearance during 2013)

OMB Clearance Number	Survey/Data Collection Name
0920-0212	National Hospital Care Survey
0920-0214	National Health Interview Survey
0920-0222	Questionnaire Development Research Laboratory
0920-0234	National Ambulatory Medical Care Survey
0920-0237	National Health and Nutrition Examination Survey
0920-0278	National Hospital Ambulatory Medical Care Survey
0920-0298	National Hospice and Home Care Survey
0920-0314	National Survey of Family Growth
0920-0404	State and Local Area Integrated Telephone Survey
0920-0729	NCHS Customer Survey
0920-0780	National Survey of Residential Care Facilities
0920-0884	Calibration of Short Strengths and Difficulties Questionnaire (SDQ) in the National Health Interview Survey
OMB-clearance exempt	National Immunization Survey

Attachment 2. Example of confidentiality pledge under CIPSEA

National Health and Nutrition Examination Survey

A. Confidentiality Brochure

The brochure contains detailed information on the confidentiality aspects of the survey including the statement **"Information gathered in NHANES is used only for statistical purposes."**

B. Signed Consent Form

You have been chosen to take part in the National Health and Nutrition Examination Survey (NHANES), held by the Centers for Disease Control and Prevention (CDC). This research tells us about the health and nutrition of people in the United States. It combines an interview with a health exam. Our interviewer will ask questions about you and your family. Some questions are about your work and general health. Others are about health problems and other health topics. Also, we will ask for your Social Security and Medicare numbers to link to vital statistics, health, nutrition and other related records so we can do research on health, nutrition and food programs. The questions today will take about one hour. We may contact you to check the work of your interviewer. We may contact you again for further studies.

We use data gathered in this survey to study many health issues. All data gathered will be kept strictly confidential. We gather and protect all data in keeping with the requirements of Federal Laws (see box below). These laws do not allow us to give out data that identifies you or your family without your permission.

You may take part in this survey or not. The choice is yours. You will not lose any benefits if you say no. If you choose to take part, you don't have to answer every question.

Do you have more questions about the survey? You can make a toll-free call to Dr. Kathryn Porter at the U.S. Public Health Service at 1-800-452-6115, Monday-Friday, 8:30 AM-6:00 PM EST. If you have questions about your rights about being in the survey, call the Research Ethics Review Board at the National Center for Health Statistics, toll free, at 1-800-223-8118. Please leave a brief message with your name and phone number. Say that you are calling about Protocol # 2005-06. Your call will be returned as soon as possible.

_____

Signature of person answering questions Date

Box:
The Public Health Service Act (42 USC 242k) authorizes collection and Section 308(d) of that law (42 USC 242m), as well as the Privacy Act of 1974 (5 USC 552A), and the Confidential Information Protection and Statistical Efficiency Act (PL 107-347), prohibit us from giving out information that identifies you or your family without your consent. Any NHANES employee or agent who violates the law may be convicted of a class E felony and imprisoned for up to 5 years, or fined as much as $250,000.

Attachment 3. Interagency Agreement for the Designation of Off-Site NCHS Agents

DEPARTMENT OF HEALTH AND HUMAN SERVICES
Centers for Disease Control and Prevention
National Center for Health Statistics

AGREEMENT BETWEEN NCHS AND [AGENCY]
REGARDING DESIGNATION OF [AGENCY] STAFF **[and contractors if applicable]** AS NCHS AGENT(S) TO PERFORM STATISTICAL ACTIVITIES USING NCHS DATA

INTRODUCTION

The National Center for Health Statistics (NCHS) conducts statistical and epidemiological activities under authority granted by the Public Health Service Act (42 USC 242k). The **[Survey]** is conducted under this authority. Pursuant to the authority granted under Title V of PL 107-347 (the Confidential Information Protection and Statistical Efficiency Act , or CIPSEA) allowing NCHS to provide access to confidential information to designated agents, the NCHS designates **[Agency]** staff who have signed this agreement as NCHS agents and agrees to provide**[access to][Agency]** a data file from **[Survey]** containing
_____ ***[identify the data file(s) to be made available including the specific information it contains that could permit identification of individuals or establishments, such as identifiers for Census region, state, county or finer geographical units.]*** A list of the variables provided is attached.

PURPOSE

The purpose of this agreement is to enable **[Agency]** to_____ **[*describe the justification and purpose of the access].*** This effort will ***[describe how this agreement will benefit NCHS and the Designated Agent].***

BACKGROUND [or PROPOSED RESEARCH or ACTIVITY]

(a) Describe in detail

- The data NCHS is providing or requesting be acquired
- The research topic or collection activities or other activities and protocol
- How the data will be used
- Any plans for disseminating information, including products planned for public distribution

DATA SECURITY AND SAFEGUARDS

1. Access, storage and disposition of the data

The **[Survey]** has been certified at a moderate level of required protection for confidentiality, integrity, and availability. **[Agency]** agrees to provide adequate security arrangements for access to, storage, and disposition of all files, extracts, printed listings; or outputs to prevent unauthorized use of these data. Security plans will comply with the requirements of the Federal Information Security Management Act (FISMA), and the Office of Management and Budget (OMB) guidelines. Documentation from **[Agency]** must be submitted to the NCHS Security Officer (ISSO) for review.

The ISSO will approve the security arrangements if **[Agency]** systems have the same level of protection for confidential data provided by NCHS.

It is understood that authorized staff of NCHS may, upon request, be granted access to premises where **[Survey]** data files are kept or used for the purpose of inspecting data security arrangements

To preclude observation of confidential information by persons other than designated agents, **[Agency]** shall maintain all **[Survey]** confidential records that identify individuals or establishments or from which individuals or establishments could be identified under lock and key. Specifically, at each site where these items are processed or maintained, all confidential and restricted-use data that may permit identification of individuals or establishments are to be kept in locked containers when not in use.

NCHS permits storage of confidential data on portable media only under extraordinary circumstances. The NCHS Confidentiality Officer must approve the use of portable media for storage of confidential information in advance. Once written approval is obtained, the medium on which the files are stored (floppy disks, CD's, DVD's, flash drives, and removable hard drives) must be encrypted and kept in locked fireproof containers or, if maintained on a computer or external hard drive, access secured by all available means (including keyboard locks, passwords, encryption, etc. and office locks).

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.

NCHS will be notified in advance of any change in **[Agency]** site access.

No confidential records may be removed from the **[Agency]**'s offices to an alternative worksite --including telecommuting worksite --or electronically accessed or sent via e-email from such a site.

2. Data Transport

All data transmissions between the **[Agency]** and NCHS must utilize **[CDC's SDN (Secure Data Network)][or describe other secure mechanism such as encrypted hard drive, etc that will be used for transmission]**. Under no circumstances should such data be transmitted through electronic mail or fax.

3. Disclosure and Confidentiality

Being aware that they are subject to all of the requirements of both the Public Health Service Act and the Confidential Information Protection and Statistical Efficiency Act of 2002, and with the understanding that violation of the terms of this agreement is subject to conviction of a class E felony, imprisonment and a fine of up to $250,000, all persons on the attached list who will be granted access to **[Survey]** agree that:

a. The NCHS data will be used only for purposes of health related research and statistical analysis. Unless specified in the agreement, no attempt will be made to learn the identity of individuals/establishments in the survey; and survey information will not be used in any way to directly affect any survey participant.

b. In accordance with the provisions of CIPSEA, the only persons to be granted access privileges to the confidential **[Survey]** data will be those who: (a) are named in the list to be provided by the **[Agency]** Data Custodian as authorized to have access to **[Survey]** data as NCHS Designated Agents; (b) have completed the NCHS Designated Agent forms; (c) have been certified as having completed the NCHS training (hyperlink to training: http://www.cdc.gov/nchs/about/policy/confidentiality_training/index.html); (d) read the NCHS confidentiality statute section 308(d) (42 U.S.C. 242m(d) of the Public Health Services Act, excerpts of Title V of PL 107-347 (CIPSEA), Section 7 of the NCHS Confidentiality Manual and the **[Survey]** assurance of confidentiality; and (e) completed the Affidavit of Nondisclosure. The person identified as **[Agency's]** Data Custodian will certify these conditions have been met.

c. No identifiable NCHS data will be released to anyone other than the persons referred to in item 2. **All requests for identifiable NCHS data from any other party will be referred immediately to NCHS. If [Agency] suspects or experiences a breach, theft, loss or potential loss of NCHS Confidential information, the [Agency] custodian named in this agreement will notify the NCHS Chief Information Security Officer, John Macias 301-458-4370 or 301-738-4769 and the NCHS Confidentiality Officer, Eve Powell-Griner 301-458-4257 or 240-505-2488 within one hour of discovering the incident.**

d. Agency's designee **[name]** will be the custodian of the files and will be responsible for the observance of all conditions of use and for the establishment and maintenance of security arrangements to prevent unauthorized use of these files. It is the custodian's responsibility to notify NCHS:

a) when access to NCHS data is no longer needed,
b) if a change in site access is contemplated,
c) of the intent to modify the project's purpose, and
d) if these responsibilities are transferred. If responsibilities are to be transferred, notification must be made promptly and before such official transfer is made.

e. At the conclusion of the project, but no later than one year from date agreement is signed **[Agency]** will either destroy or return to NCHS all data files, backup files, or derivative files containing **[Survey]** data that could permit identification of individuals or institutions. Official confirmation will be provided by the **[Agency]** data custodian named in item 4 above, of their return/destruction by completion of Attachment D, Part C within 30 days of the agreement expiration. Should **[Agency]** require additional time, a new agreement may be negotiated subject to approval of the NCHS Confidentiality Officer. ***[Note: unless significant change is contemplated, the new agreement may take the form of a simple memo, but should be initiated at least one month prior to the termination of the exiting agreement. See attachment J].***

f. All reports based on **[Survey]**, will be submitted prior *to public release* (whether as oral presentation, papers or publications) to the NCHS program representative for disclosure review. Failure to do so will be considered a violation of this agreement and access to **[Survey]** data will be immediately terminated.

g. The NCHS program representative for this project is **[name]**.

Director, **[AGENCY]**

_____	_____	_____
Print name	Signature	Date

Director, National Center for Health Statistics

_____	_____	_____
Print name	Signature	Date

Confidentiality Officer, National Center for Health Statistics

_____	_____	_____
Print name	Signature	Date

Program Representative, National Center for Health Statistics

_____	_____	_____
Print name	Signature	Date

Designated Agents, **[AGENCY]**

Custodian

_____	_____	_____
Print name	Signature	Date

Other Agents **[attach list if necessary]**

_____	_____	_____
Print name	Signature	Date

_____	_____	_____
Print name	Signature	Date

I have reviewed the security plans of [Agency]. These plans comply with the security requirements of FISMA, OMB guidelines, and CDC policy. The documentation from [Agency] indicates that the security system provides the same level of protection of confidential data as that provided by NCHS.

_____ Date:_____

NCHS Information Systems Security Officer

Designated Agent Information

Name (print): last, first, middle Date of Birth: month day year

_____

Local home address: street, city, state, zip code

_____

Legal address (if different from above) street, city, state, zip code

Home telephone number_____ Cell telephone number_____

Citizen of the United States ___ ___ If not, Citizen of _____
Yes No

_____ _____
(signature) (date)

Date NCHS Training Completed: _____ Confirmed by:_____
Signature of Agency Custodian

Affidavit of Non-Disclosure

I,_____, do solemnly swear (or affirm) I will observe all policies and procedures to protect the confidentiality of data collected as set forth in the attached agreement between the National Center for Health Statistics and _____) and that I will not disclose confidential information, either while an agent or after, contained in data files, lists, or reports created using National Center for Health Statistics data, as specified under Section 308(d) of the Public Health Service Act and under penalties set forth in §513 of the Confidential Information Protection and Statistical Efficiency Act of 2002 (PL 107-347, title V), 44 USC 3501 note.

_____
(Signature of Designated Agent)

Subscribed and sworn (or affirmed) before me this ____ day of _____, 20__.

At_____(city) _____ (state)

[SEAL] _____
(Signature)

My commission expires_____ Title (Officer/Notary Public) _____

Note: The oath of non-disclosure must be administered by a person specified in 5 U.S.C. §2903. The word "swear," wherever it appears above, should be stricken out when the appointee elects to affirm rather than swear to the affidavit; only these words may be stricken, and only when the appointee elects to affirm the affidavit.

Certification of Destruction of NCHS Data Files

Note: To be completed by the agency custodian and returned to NCHS within 30 days of agreement expiration date.

Designated Agent Agreement Expiration Date: _____

As the [Agency] custodian for the [insert project name], I affirm that all electronic and paper files for this project have been destroyed. The individual file names and data years are listed below:

File Name	Data Year(s)
_____	_____
_____	_____

(attach additional pages if needed.)

All derivative and back-up copies have been destroyed. Yes ___ No____ If no, state reason below:

_____

_____

_____ _____ _____

Data Custodian printed name and title | Signature | Date

Return this signed form to the NCHS Program Representative [name and address]

_____

Upon receipt at NCHS:
I [insert NCHS program representative] certify that the list of files above includes all files provided by NCHS under the terms of this agreement.

_____ _____

Signature | Date

NOTE: Provide a copy of this completed form to the NCHS Confidentiality Officer

NCHS CONFIDENTIALITY LEGISLATION:

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

> ‘‘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.’’

CIPSEA LEGISLATION

Title V of PL 107-347 (The E-Government Act of 2002) – Confidential Information Protection and Statistical Efficiency Act of 2002 (CIPSEA):

> “Data or information acquired by an agency under a pledge of confidentiality for exclusively statistical purposes shall be used by officers, employees, or agents of the agency exclusively for statistical purposes……. (The data) shall not be disclosed by an agency in identifiable form, for any use other than an exclusively statistical purpose, except with the informed consent of the respondent.”

Concerning fines and penalties, the act states that:

> “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.”

NCHS MANUAL ON CONFIDENTIALITY

Section 7 of the NCHS Staff Manual on confidentiality

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 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 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) is not permitted except in unusual circumstances and with written prior approval of the Director of the data division owning the data, the immediate supervisor, and the NCHS Confidentiality Officer. Such applications include *all* cases where confidential data would be accessed from outside NCHS offices *and are not limited to flexiplace requests*. If use of in-house files is approved, the staff member must agree in writing not to download the contents of confidential files accessed from home or from an alternate work site. If use of in-house files is approved, confidential files placed on laptop computers must be encrypted using CDC approved software. 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 traceable means available (e.g., Fed Ex, personal messenger, or directly by NCHS staff).

H. Confidential data 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 Information Systems Security General

Identifiable NCHS data are considered highly sensitive. In achieving the goals of the Privacy Act of 1974, the Confidential Information Protection and Statistical Efficiency Act of 2002 (CIPSEA), and OMB Circular A-130, policy and guidance documents have pointed to the important area of information systems security in establishing safeguards to ensure the security and integrity of records. Adequately protecting confidential information from disclosure requires adequate security for information technology (IT) systems as well as physical security for information storage.

The DHHS-OCIO Policy for Information Systems Security and Privacy[1] ("the Policy") is a Departmental directive which provides practices and procedures intended to carry out OMB Circular A-130, and regulate the security of Federal information resources. Appendix A of the Policy, *HHS-OCIO Policy for Information Systems Security and Privacy Handbook* ("the Handbook"), outlines requirements for IT security and privacy programs and information systems in detail.

CDC is required by OMB Circular A-130, Management of Federal Information Resources[2] to:

> "Protect government information commensurate with the risk and magnitude of harm that could result from the loss, misuse, or unauthorized access to or modification of such information."

CDC's information technology security program[3] contains additional requirements applicable to all CDC information systems. "Information systems" is defined as any information system that supports the operations and assets of the agency and includes desktop PC workstations, laptop computers and other mobile devices, portable media, servers, network devices, and office automation equipment such as copiers and fax machines.

All persons who control, handle, or use the data share responsibility for the security and integrity of the records, including system/network administrators, the Information Systems Security Officer, systems analysts, programmers, data preparation personnel, and IT systems users. Contractors who access 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.

---

[1] See: http://www.hhs.gov/ocio/policy/hhs-ocio_policy_for_information_systems_security_and_privacy__.html

[2] See (http://www.whitehouse.gov/omb/circulars/a130/a130trans4.pdf)

[3] See http://aops-mas-iis.cdc.gov/Policy/Doc/policy300.pdf

Information systems security. All systems users should familiarize themselves with the contents of the DHHS and CDC information systems security policies and guidelines and comply with the requirements. The basic requirements for all individuals using CDC systems are summarized below.

h. Complete required privacy and information security refresher training
i. Read, acknowledge, sign (if online completion is not available), and comply with the HHS Rules of Behavior, as well as other applicable CDC- and system-specific rules of behavior before gaining access to the CDC's systems and networks
j. Adhere to the requirements set forth in the *CDC IT Security Program Implementation Standards*, and other security policies and procedures that minimize the risk to CDC systems, networks, and data from malicious software and intrusions
k. Abide by all applicable acceptable use policies and procedures, including the *Use of CDC Information Technology Resources* policy, regarding use or abuse of CDC IT resources
l. Seek guidance from your supervisor when in doubt about implementing policy documents
m. Know which systems or parts of systems for which you are directly responsible (e.g., desktop, computer, laptop computer, attached printer, etc.)
n. Ensure that adequate protection is maintained on your workstation, including not sharing passwords with any other person and logging out, locking, or enabling a password-protected screen saver before leaving your workstation Refrain from loading any software on CDC systems or networks unless the software is on the CDC-approved list, and only installed by individuals with specific permission from management and information security personnel
o. Ensure that all media containing CDC data are appropriately marked and labeled to indicate the sensitivity of the data, in accordance with CDC policy for protecting sensitive information
p. Do not disable, remove, install with intent to bypass, or otherwise alter security settings or administrative settings designed to protect Department IT resources
q. Use approved encryption methods wherever applicable to protect sensitive information on computers, on portable media, and during electronic transmission
r. Know the security category of the data you handle and familiarize yourself with any special requirements for accessing, protecting, and using the data; this includes, but is not limited to, the Privacy Act requirements, copyright requirements, and procurement-sensitive data
s. Immediately report any suspected or actual computer incidents (including loss of PII) to your supervisor, Information System Security Officer (ISSO), NCHS Confidentiality Officer, and the CDC Computer Security Incident Response Team (CSIRT) in a timely manner, and cooperate in the investigation of incidents.

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 files;
F. Documentation production run procedures; and
G. Documentation related to statistical disclosure limitation procedures and disclosure review.

Certification of Completion of Confidentiality Training and Nondisclosure Affidavit

I certify that persons named in the attached list as authorized to work with the data from [Survey] have:

a. Seen the NCHS Confidentiality Videotape or reviewed the provided confidentiality training materials;
b. Read the NCHS Confidentiality Statute (42 U.S.C. 242m(d) and CIPSEA;
c. Read Section 7 of the NCHS Confidentiality Manual pertaining to Protection of Records and Data Systems;
d. Read the [Survey] assurance of confidentiality; and
e. Have signed the NCHS Nondisclosure Affidavit

_____ Date:_____

Agency Custodian Signature

Attachment 4. NCHS On-site Designated Agent (including RDC)

(to be completed by NCHS staff and researcher)

(As required by the Privacy Act of 1974, the personal information being requested will be kept confidential and will be used only for the purpose of identifying a researcher who may be granted designated agent status. Providing the information is strictly voluntary; however, not providing it will prevent you from being considered for agent status.)

Part A

_____ _____

Name: last, first middle Date of Birth: month day year

Social Security Number (Last four digits only)_____

_____

Local home address: street, city, state, zip code

_____

Legal address (if different from above) street, city, state, zip code

Home telephone number_____ Cell telephone number_____

Employer _____ Supervisor _____

Work address _____

Telephone number _____ Supervisor's telephone number _____

Citizen of the United States ___ ___ If not, Citizen of _____

Yes No

Part B

Reason for access to NCHS confidential files:

_____

_____

_____

How long is agent expected to require access to NCHS confidential files:

From ___ ___ ___ To___ ___ ___

Mo Day Yr Mo Day Yr

NCHS employee supervising Designated Agent_____ _____

(signature) (date)

Confidentiality Officer _____ _____

(signature) (date)

Part C

Affidavit of Non-Disclosure for on-site NCHS Designated Agent

I,_____, do solemnly swear (or affirm) I will observe all policies and procedures to protect the confidentiality of data to which I will have access and that I will not disclose confidential information, either while an agent or after, contained in data files, lists, or reports created using National Center for Health Statistics data, as specified under section 308 (d) of the Public Health Service Act and under penalties* set forth in §513 of the Confidential Information Protection and Statistical Efficiency Act of 2002 (PL 107-347, title V), 44 USC 3501 note.

_____
(Signature of Designated Agent)

Subscribed and sworn (or affirmed) before me this ____ day of _____, 20__.

At_____(city) _____ (state)

[SEAL] _____
(Signature)

My commission expires_____ Title (Officer/Notary Public)_____

Note: The oath of non-disclosure must be administered by a person specified in 5 U.S.C. §2903. The word "swear," wherever it appears above, should be stricken out when the appointee elects to affirm rather than swear to the affidavit; only these words may be stricken, and only when the appointee elects to affirm the affidavit.

*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.

Attachment 5. Example of Contract Language

3.1.4 Task 4: Regulatory Support-Confidentiality/Security

Confidentiality procedures for contractor personnel:
All information made available to the contractor while performing this task, both electronic and otherwise, shall be maintained in a strictly confidential manner.

Contractor personnel performing this work may have access to information that is subject to provisions of the Privacy Act of 1974 (Title 5 of the U.S. Code, Section 552a), Section 308(d) of the Public Health Service Act (42 USC 242m) and the Confidential Information Protection and Statistical Efficiency Act (CIPSEA, PL 107-347). Violation of the CIPSEA is subject to conviction of a felony and fines of up to $250,000. Contractor personnel shall adhere to appropriate nondisclosure requirements.

Additionally the Contractor shall comply with the following NCHS policies:

- Safeguards for Individuals and Establishments against Invasion of Privacy

  In accordance with Subsection (m) of the Privacy Act, Section 308(d) of the Public Health Service Act, and the CIPSEA, the contractors, and employees of the contractor, are required to undertake 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 USC 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."

  Annually and for every new hire that occurs during the period of performance, the contractor is required to have each employee of the contractor participating in this project, read and sign the nondisclosure affidavit (Attachment 1), which indicates he/she has carefully read and understands the assurance which pertains to the confidential nature of all records to be handled in regard to this survey and he/she has viewed the mandatory DVD "NCHS Confidentiality Practices for Federal Employees and Contractors". All of the signed nondisclosure affidavit must be sent to the Technical Support person at NCHS listed on page 1 of this SOW. NCHS will be notified immediately of any new hires during the period of performance and the signed nondisclosure affidavit will be sent to NCHS as described above. Attachment 2 (Commonly Asked Questions Concerning Confidentiality at NCHS) and Attachment 3 (Executive Summary of the NCHS Confidentiality Manual) are referenced in the affidavit.

  As an employee of the contractor, he/she understands they are prohibited by law from disclosing any such confidential information, which has been obtained under the terms of this contract to anyone other than authorized staff of NCHS.

  The contractor and his professional staff will take steps to insure that the intent of the statement of understanding is enforced at all times through appropriate qualifications standards for all personnel working on this project and through viewing of the DVD "NCHS Confidentiality Practices for Federal Employees and Contractors", the Commonly Asked Questions Concerning Confidentiality at NCHS, the Executive Summary of the NCHS Confidentiality Manual, and signing the NCHS Nondisclosure affidavit that will be provided to the contractor by NCHS and periodic follow up procedures.

- **Security Requirements**:

The contractor must comply with HHS-OCIO Standards for Security Configurations, HHS Standard 2010-0001.015; see Attachment 4 of this PWS. The contractor will 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, at each site where these items are processed or maintained, all PII Data (Personally Identifiable Information) i.e. confidential records that will permit identification of individuals or establishments, are to be kept in locked containers when not in use by the contractor's employees. The keys or means of access to these containers are to be held by a limited number of the contractor's staff at each site.

If records are maintained in electronic form, the medium on which the files are stored (floppy disks, CD's, DVD's, flash drives, and removable hard drives) must also be kept in locked fireproof containers or, if maintained on a computer or external hard drive, access secured by all available means (including keyboard locks, passwords, encryption, etc. and office locks). Electronic storage of SSN's must be encrypted with a Federal Information Processing Standard (FIPS) approved product (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm).

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.

NCHS will be notified of any change in contractor site access and the contractor will provide to NCHS, a new System Security Plan (SSP) according to National Institute of Standards and Technology (NIST) SP 800-53 guidelines for a low-rated system.

No confidential records may be removed from the contractor's offices to an alternative worksite including telecommuting work site or electronically accessed or sent via e-email from such a site.

All data transmissions between the contractor and NCHS must utilize CDC's SDN (Secure Data Network). Under no circumstances should such data be transmitted through electronic mail or fax.

Copies of confidential records (paper documents, electronic files, video records, or records of other kinds) are not to be made, except as needed for operational purposes. At the end of the period of performance, and possibly at various completion points in the contract, NCHS will issue a formal request to the Contractor that data received and generated during the period of performance (including the original input, copies, backups, and generated output) be destroyed. At this time, the Contractor will permanently delete all copies of the data referenced in the NCHS request and provide written verification to NCHS (within 30 days of the request) that the data has been destroyed

Legal authority and privacy law applicability: The Contractor and its employees are subject to criminal penalties for violation of the Privacy Act to the same extent as employees of the Government. The Contractor shall assure that each of its employees knows the prescribed rules of conduct and that each is aware that he or she can be subjected to criminal penalty for violation of the Act. A copy of the Privacy Act Regulation is located at the following Internet Site: http://law2.house.gov/uscode-cgi/fastweb.exe?search. If preferred, a copy of the Privacy Act Regulation can either be e mailed or sent through the mail.

The Privacy Act monitor is the NCHS/DHIS Project Officer, who may confer with the NCHS Privacy Official as necessary. The Privacy Act System of Record number is 09 20 0164.

Contractor employees assigned to this task shall sign and adhere to the NCHS Confidentiality Pledge provided by the NCHS/DHIS Project Officer.