ADDM Network

Data Confidentiality and Security Agreement

Updated – May 2011

ADDM Network Data Confidentiality and Security Agreement

ADDM Surveillance Data Confidentiality and Security Agreement

Table of Contents **Page**

ADDM **Network Data Confidentiality and Security Agreement**

I. Confidentiality Security Statement for the ADDM Network

This agreement applies to individuals collecting or using data as part of the Autism and Developmental Disabilities Monitoring (ADDM) Network. The guidelines are required to be minimal standards for all ADDM sites; however, any site may adopt additional guidelines that are more stringent and adhere to the guidelines of their home institution. If the guidelines of your home institution are incompatible with these guidelines, it is necessary to contact the ADDM Project Coordinator and the site Technical Steward for resolution.

This document describes the procedures and practices each site in the ADDM Network is required to use to protect the confidentiality of the data collected or distributed as part of this surveillance activity funded by the Centers for Disease Control and Prevention (CDC)/ National Center on Birth Defects and Developmental Disabilities (NCBDDD). The ADDM Network Project Officer is Victoria Wright (email: vwright@cdc.gov), NCBDDD/CDC. The ADDM Project Coordinator is Anita Washington (email: czo9@cdc.gov), RTI/NCBDDD/CDC. The ADDM Co-Principal Investigators are Jon Baio (jbaio@cdc.gov) and Cathy Rice (crice@cdc.gov). Any questions regarding IT security procedures should be sent to Andy Autry (AAutry@cdc.gov) with cc to Anita Washington. The primary contact for each ADDM site is that site's Principal Investigator(s). The Confidentiality Designee and Technical Steward should also be included in all discussions of site-specific confidentiality concerns.

Project personnel (defined in this document as all ADDM Site staff and contractor staff, guest researchers, fellows and research assistants or other personnel who have approved access to identifiable project data) are required at all times to maintain and protect the confidential records that may come into their presence and under their control according to these guidelines and any additional site guidelines, as applicable (please see Attachment A2- Our Responsibility to Protect Personal Information (HHS – Staff document)

All documents, paper and electronic, for the ADDM Network containing names and other information identifying a single individual or a single institution and other project files, will be considered confidential materials and will be safeguarded to the greatest extent possible. Because the data are highly sensitive, the security requirement is rated as high. It is the professional and legal responsibility of each individual associated with this project to protect the right to confidentiality of the individuals (i.e. children and their families) in the project database, project offices, and any other location of these records.

Extra precaution should be taken to protect the security of the 18 identifying variables cited in the Health Insurance Portability and Accountability Act (HIPAA). The following are 18 HIPAA identifying variables:

1. Names;
2. All geographic subdivisions smaller than a State; including street address, city, county, precinct, zip code, and their equivalent geocodes; except for the initial three digits of a zip code if according to the current publicly available data from the Bureau of the Census:
    - The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
    - The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people are changed to 000.
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
4. Telephone numbers;
5. Fax numbers;
6. Electronic mail addresses;
7. Social security numbers;
8. Medical record numbers;
9. Health plan beneficiary numbers;

10. Account numbers;
11. Certificate/license numbers;
12. Vehicle identifiers and serial numbers, including license plate numbers;
13. Device identifiers and serial numbers;
14. Web Universal Resource Locators (URLs);
15. Internet Protocol (IP) address numbers;
16. Biometric identifiers, including finger and voice prints;
17. Full face photographic images and any comparable images; and
18. Any other unique identifying number, characteristic, or code, except as permitted by number three of this section; and
    - The covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

II. Safeguarding Measures and Restrictions on Use of Information

A. Confidentiality Designee and Training

Each site must identify a Confidentiality Designee who will receive training on these guidelines from the ADDM Project Coordinator, Anita Washington. Once a site has their designated Confidentiality Designee, that person is responsible for the initial and annual training of other staff members at that site. All project staff working on this project will be required to attend a training session to review these guidelines and the confidentiality issues particular to this project, and sign the Confidentiality Statement of Understanding. This training must take place before any site or individual has access to project confidential data or begins to collect identifiable data. The Confidentiality Designee will be responsible for ensuring all site personnel are trained in data confidentiality and security, and that these materials are reviewed on an annual basis. Each site must ensure that there is always a Confidentiality Designee, and changes in assignment of this duty must be communicated to Anita Washington immediately.

During the annual training the confidentiality designee is required to review the agreement with staff, discuss any new guidelines or technology changes, and ask the staff to sign a new Confidentiality Statement of Understanding. Sites can also require any site specific training that may be required for their specific institution.

B. Confidentiality Statement of Understanding for ADDM Staff

To assure that all ADDM staff are aware of this responsibility and the penalties for failing to comply, all project personnel who have access to identifiable information related to the projects must read and sign the Confidentiality Statement of Understanding, assuring that all identifying information will be kept confidential and will be used only for epidemiologic or statistical purposes.

Attachment A1 is the Confidentiality Statement of Understanding for ADDM Staff.

Signed agreements will be obtained by the site's confidentiality designee and maintained in the employee's file. Each site's principal investigator or confidentiality designee must review these and any additional security requirements of that site before any access to identifiable data is granted to the employee. The originals should be retained in files at the project site and readily accessible upon request.

C. Restrictions on Use of Information

1. Information collected or retrieved by project personnel in the course of conducting the project will be used only for the purposes of carrying out project activities and shall not be divulged or made known in any manner unless approval from the project participant is received (written notice and data source director approval). This information is to be sent by the PI or PC.
2. Project staff are responsible for protecting all confidential records from visual observation,

from theft, or from accidental loss or misplacement due to carelessness. All reasonable precautions will be taken to protect confidential data. Project staff shall not conduct any work with confidential data while using public transportation, **using open access (no ID required to access internet) public internet**, or using any other public venue that could be accessed by individuals not working with the project.

3. CDC requires any materials (written or electronic) containing personal identifiers that must be sent to authorized project personnel should be sent via first class certified-return receipt mail or commercial carrier service in a sealed envelope stamped "CONFIDENTIAL" on the front.
4. CDC does not recommend the electronic transmission (via fax, text, or e-mail) of records or data containing names or other personally identifying information. However, if an ADDM site deems it is necessary and allowable to transmit personally identifiable data electronically, they should follow the HIPAA Standard to implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. (**4.18 Transmission Security (§ 164.312(e) (1)).** At a minimum, any information e-mailed with identifiers should be encrypted with (FIPS) 140-2 compliant software and all precautions taken to ensure that fax machines are in a secure location and are retrieved only by authorized personnel. Text messaging is not allowed for electronic transmission of records or data containing names and other personally identifying information.
5. Project personnel are not to divulge any personal identifying information about project participants to anyone other than authorized project staff on a "need to know" basis appropriate to conduct official business. In general, conversations outside the workplace, neither the identifying information, specific details about the data collected, nor the means by which they are collected should be discussed in any detail. Breach of confidentiality due to project personnel knowingly and willfully disclosing confidential information may result in removal from the ADDM project. If a breach of confidentiality is due to unintentional, but careless behavior and/or not following guidelines to maintain confidentiality of data, the behavior will result in, (at a minimum), a temporary removal from accessing confidential information, and site-specific sanctions will apply. CDC may make a recommendation but permanent reassignment to another project is at the discretion of each ADDM site and in conjunction with site-specific personnel guidelines (refer to Section IV. 2 for more information).
6. When not in use by authorized project staff, all hard copy material and physical media containing confidential data will be stored in locked containers, locked file cabinets, or locked rooms. Access to locked storage areas will be limited to authorized project staff. This procedure will apply to all physical media containing confidential data, including data collection forms, printouts, diskettes, CDs, flash drives, laptop computers, and magnetic data tapes. Staff working with confidential materials during forms processing and data handling will have access only to the materials that they are currently processing. When confidential records are in use, they must be kept out of sight of persons not authorized to work with these records. For individuals who are working at home or traveling, all hard copy confidential data must be secured. ADDM staff should only use laptops/desktops provided by the project to access data.
7. Except as needed for operational purposes, photocopies of confidential records are not to be made. If photocopies are necessary, care should be taken that all copies and originals are recovered from the copy machines and work areas. All confidential paper records will be destroyed as soon as operational requirements permit by burning or shredding the documents.
8. No data (or copies of data) are to be retained by a contractor after completion of the period of performance of the contract, or as specified in the contract for reasonable handling of data on back-up tapes/drives. ADDM staff should make sure that all data is secure by storing data in

locked filing cabinets or containers. It is also required to either shred all project related documents or return them to the project coordinator once the study year has been completed. ADDM staff should take special precaution to avoid working in public places with any of the confidential data.

9. Unless specifically instructed otherwise for a particular project approved by the Principal Investigator, employees will not be allowed to abstract, collect or process data from a respondent whom they know personally.
10. Please see Attachment A2 that provides additional precautions for protecting personal information from the HHS Chief Information Officer. It is required that all ADDM staff adheres to these precautions.

D. Enhanced Protection of Computerized Files

In addition to any documents and materials, all project data maintained in electronic storage systems will be protected to maintain confidentiality. The following safeguards shall be implemented to protect files so that the accuracy and the confidentiality of the data can be maintained:

1. **ADDM Grantee Sites:**
   a. Electronic data files will only contain names or other personal identifiers (other than the project identification number) when absolutely necessary for project purposes. Any electronic data that is sent must be encrypted and password protected.

   b. Printed data files for clinician review should only contain evaluation dates. No other personal identifiers should be listed on the report.

   c. Personal identifiers entered electronically and housed in a secure project location will be stored in data files that will be maintained under password-protected computer accounts and encrypted. All personal identifiers that are carried on laptop computers into the field will be encrypted and password protected.

   d. Computer files containing programs, documents, or confidential data will be stored in computer systems that are protected from accidental alteration and unauthorized access. Computer files, whether they are stored on a mainframe computer, a LAN or individual computers, will be protected by password systems, controlled sharing, and routine daily (or site specific) backup procedures. It is required that all laptops have third party encryption software. Backup files will be stored in secure off-site facilities. Computer facilities at all sites will be protected from potential fire or water damage.

   e. Never share passwords with other individuals, including family members. Change temporary passwords at the first log-on. Change passwords on a regularly scheduled basis or if a password has been compromised (e.g. was shared with an IT person for computer maintenance). Do not reuse old passwords within 3 password changes. Use strong passwords that contain upper- and lower- case letter, characters, numbers, and are not real words or numbers associated with the individual.

   f. No personally identifiable data should be stored on a portable data storage device, such as a floppy disk, compact disc (CD), USB flash drive, or other such devices unless the data contained within can be encrypted to the (FIPS) 140-2 standards for the National Institute of Standards and Technology (www.nist.gov).

   g. Install and use firewalls on all computers.

   h. Install antispyware and antivirus software and keep it turned on and up-to-date.

i. Recommend password protection on cell phones (enter a password to retrieve voicemail.)

j. Emails containing personal identifiable information may not be auto forwarded to an account not affiliated with the site's home institution, including but not limited to personal and commercial email accounts such as gmail, Yahoo, or MSN. Be aware that accessing email from personal computers (one owned by the staff member) can result in automatic storage of files on that computer. Take measures to ensure appropriate security with these files. It is recommended that email should not be accessed from a personal computer. Do not click links contained in emails or open email attachments unless from a trusted site.

k. In addition to these guidelines, all sites should comply with the data security and storage agreement of their institution. It is required that each site maintains documentation of all their data security procedures, software, and equipment used to maintain these policies.

2. **Information Technology (IT) Security Procedures for the ARCHE Database**

Since the ARCHE database includes data that may contain personal identifiers, these procedures are required for all users and data administrators/managers for the ARCHE database system, and should be implemented by qualified computer support personnel at all ADDM sites, including CDC (MADDSP). Sites not using the ARCHE database should follow the minimal guidelines to protect data outlined in the section above. Any questions regarding IT security procedures should be sent to Andy Autry (AAutry@cdc.gov).

a. **Power On Password** – This is a CMOS power on password to be initiated for all laptops containing the ARCHE system. It can be set through the CMOS menu at booting and is required on all laptops.

b. **Windows 7/XP/Vista** – This is a logon password which should correspond to the network password for most laptops that grants access to the laptop and the Windows managed components. This is required on all laptops.

c. **Screen Saver Security –** Users should implement a screen saver password, so that, when any computer with ARCHE or other ADDM-related confidential data is left idle (not being used by authorized project personnel), a password-protected screen saver will automatically engage. On the computer desktop, right-click in any open space and select Properties. On the Properties window, select the Screen Saver tab. Select the desired screen saver from the drop-down list, select a Wait time, and check the checkbox for "On resume, password protect". Any time a user leaves a secured computer containing ARCHE or confidential data for any period of time, (rather than allowing the computer to wait the specified period of time before engaging the screen saver) that user should press Ctrl + Alt + Delete on the keyboard, and select Lock Computer from the window which appears. When the user returns to the computer, the user can press any key and enter the password to unlock the computer. Remember a laptop should never be left unsecured without the staff person having direct supervision of the equipment.

d. **MS Access Workgroup Security** – This is the workgroup file which contains the login id and password to grant access to the data stored in ARCHE. CDC requires that each site purchase a USB flash drive of no less than 64 MB. It is recommended for the workgroup flash drive be encrypted and strongly recommended to use additional biometric flash drives with fingerprint authentication. The workgroup file should be placed on the flash drive and the shortcut rewritten so that it points to the correct drive letter (Windows 7/XP/Vista will automatically map the drive letter upon insertion of the flash drive). CDC requires any replica (or back-up copy) of the ARCHE database or other personally-identifiable data should be placed on an encrypted flash drive that is separate from the workgroup flash drive. The workgroup flash drive must be in place at all times when ARCHE is in use and

remain under direct supervision of the person using ARCHE. Both flash drives should be kept separate on the employee's person during transportation and must not be stored with the laptop at anytime. When not in use, both flash drives must be stored separately in a secured location. The flash drives should not be stored in the same location as the laptop when not in use. The flash drive containing the workgroup file should not also contain replicas or back-ups of the ARCHE database or other personally-identifiable data.

e. **MS Access Encryption** – This is encryption of the physical database which should prevent hackers from using a Windows tool, text editor, or other cracking mechanism to compromise the data on the laptop.

f. **Third Party Encryption Software** – CDC requires that each site purchase commercial "off the shelf" encryption software that meets the National Institute of Standards and Technology (NIST) Federal Information Processing System (FIPS) 140-2 Standards capable of encrypting/decrypting folders "on the fly" (dynamic encryption allowing single entry of password for decrypting/encrypting at folder or disk level). This encryption software should be utilized on all computers containing the MS Access and using the ARCHE database, so that any copy of ARCHE can be encrypted. It is required that the entire hard drive is encrypted, so that any data on the drive are protected (including the recycle bin, etc.). Estimated costs $150 -$250 for an encryption software meeting the above standards. Specific products are not recommended but the above requirements are necessary to work with the ARCHE database.

g. **Backup of ARCHE Database** – All backups of the ARCHE database must be encrypted (either encrypted with third party software and burned to CD or flash drive or saved to an encrypted flash drive). The encryption software must be (FIPS) 140-2 compliant.

h. **If it is necessary to abstract individual Social Security Numbers (SSNs), only the last 4 digits should be stored in ARCHE and labels such as "SS" or "SSN" should not be used**. Alternative identifying acronyms include "Child Identification Number" (CHID) or "Mother Identification Number" (MID).

E. Dissemination of Research Results

Unless specific parental consent is granted to share identifiers with approved entities, all reports and publications of collected project data will be presented in aggregate form only. The names or other identifiers (see 18 identifying variables on pg.3) of participating individuals will not be presented in any publication. Reports will be written so that no person may be individually identified, even indirectly. Reporting of aggregate data will be sensitive to adhere to guidelines of the National Association of Health Data Organizations "Statistical Guidelines for Small Numbers" (www.nahdo.org/hidsc/datareleaseguidelines.aspx).

There can be circumstances when data provided by a source containing identifiers are given back to that source, but these agreements for datasharing must make sure that no identifying information that the source did not already have access to be given back to that source. Any site that has a specific agreement to share data back with a source or an individual must follow all site-specific data protection and Institutional Review Board (IRB) Guidelines, as appropriate, to maximize protection of confidential data.

F. Data Sharing with Other Project Partners

Project data that are to be pooled for the ADDM Network will be sent to the CDC without identifying variables, (as agreed upon by the ADDM Projects). The CDC will not release any data without the approval of the ADDM PI Datasharing Committee.

Individually identified data on individuals or establishments (sources, diagnosticians, etc.) will only be shared across project sites or with non-project personnel upon specific approval of the site's

appropriate Institutional Review Board(s) (IRBs) (as appropriate) for a specific data collection or analysis purposes. The project must be in line with the original purpose for which the project data have been collected, or re-review by local IRB(s) might be necessary. The CDC Lead/Advisor (Cheryl Coble, email: ccoble@cdc.gov) should be consulted if there are requests that present unusual circumstances or appear problematic. In addition, all sites should reference the "ADDM Datasharing Guidelines" (posted on SiteScape) for additional guidance. There should be no datasharing of the 18 identifying variables cited in the Health Insurance Portability and Accountability Act (HIPAA) (see Section I of this document for a list of these variables) without the approval of Principal Investigator's Datasharing Committee and Guidelines, local IRBs and MOU agreements (as appropriate). CDC is required to make the data publicly available within one year following final data cleaning procedures.

III. Instructions to ADDM Personnel Concerning Confidentiality Procedures:

A. General Procedures:

1. All ADDM staff that will have any access to confidential data will be required to sign a Confidentiality Statement of Understanding. This pledge must be signed annually by all project staff.

2. Use of confidential data, including abstraction, data entry, and other activities, should always be conducted in the most private setting available. When at a site, please try to complete your work in a secure location. If a private space is not available please try to limit the amount of information you have out at one time, be aware of who is in your surroundings, and take precaution to protect the confidentiality of the data. Do not access any confidential data when you are using public transportation, **using open access (no ID required to access internet) public internet**, or using any other public venue that could be accessed by individuals not working with the project.

3. Treat materials containing confidential information as your own sensitive information, such as a driver's license or credit card, and make sure the materials are always in your sight or secured properly.

4. It is the employee's responsibility to make sure that all project materials in his or her possession are protected from loss or theft to the maximum extent possible.

5. Keep a copy of your laptop's serial number and store it in a safe place away from the laptop case.

6. Never store passwords or other identifiable information with your laptop. Do not store flash drives containing the workgroup file to the database or confidential material in the same location as the laptop.

7. All ADDM and CDC staff who share work space should use extra precaution to protect any project materials from loss or theft. Please make sure that all work stations are completely locked and secured before leaving at any time.

B. Office Procedures On-Site:

1. When paper records or computer screens that contain confidential information are in use, they must be kept out of sight of persons not authorized to work with these records. For example, documents containing personal identifiers should be placed with identifiers face down on desks or surfaces where unauthorized individuals might see them.

2. When using computers or laptops containing confidential data, make sure to activate the

password lock when leaving the work area, even if for a short while such as to use the restroom.

3. Keep the flash drive required to access the ARCHE workgroup file on your person or secured at all times. Do not store the flash drive in the same location as the laptop or other computer. When not in use, store your flash drive in a secure location. The flash drive containing the workgroup file should not also contain replicas or back-ups of the ARCHE database or other personally-identifiable data.

4. Keep all computers containing files with confidential data in a locked room or area designated for project confidential data when not in use.

5. Lock all file cabinets and offices after business hours and when project staff are away from the office for extended periods of time (i.e., do not leave paper records, diskettes, CDs, flash drives, or laptop computers containing confidential information on the desk). Make sure laptops are locked down or in a secure container when not in use.

6. CDC recommends the use of security cables for laptop computers at all times. CDC is not recommending a specific product, but a cable lock that can be used at a desk or any location with the laptop. An example of what MADDSP is using can be found at: www.dell.com, http://accessories.us.dell.com/sna/productlisting.aspx?c=us&l=en&cs=19&category_id=5500&brandid=200&first=true.

Targus Lock Cable	A04249436 (Dell)	$35.00
For laptops	PA41U (mfg)	

7. Promptly and thoroughly destroy all confidential paper records as soon as operational requirements permit by cross shredding or burning the documents. In addition, all electronic and/or scanned files should be deleted from your flash drive and computer.

C. Field Procedures for Abstraction Staff Traveling in the Field

1. When traveling in the field, use a secure briefcase or computer carrier with a locking mechanism to carry the laptop, project equipment and hardcopy materials containing data. Keep the briefcase locked at all times while traveling from one location to another. Make sure the briefcase is in your sight or in a secure location at all times. Note that the flash drive containing the workgroup file that enables access to the ARCHE database should be kept in a separate, secured location from the laptop carrier (on your person, in another secure case).
2. When traveling in a vehicle, conceal all project materials, including the laptop, in the locked briefcase in the trunk of your vehicle or shielded from sight (in the case of a vehicle without a trunk) rather than in the passenger area. If you must temporarily store these when traveling by vehicle from one location to the other, lock the project materials in your trunk or out of sight, but do not leave them unattended for any extended length of time (especially, for long periods, overnight, etc.). If you are traveling overnight and staying in a hotel or other location, make sure all project materials and your laptop are either with you or locked in a secure location. Do not leave your laptop in your vehicle overnight or out in the open in a hotel room.
3. Limit the number of stops when traveling between data sources and your secure office or storage location.
4. When you have completed your field abstraction for the day, the secure briefcase or carrier and project materials, including laptop, should be returned to your place of employment, home office, or secure work area. Do not leave the secure briefcase or project materials in your vehicle when not in use.

5. Before taking a copy of confidential information into the field (i.e. a copy of database on a laptop) make sure that the site has performed database back up and replication as scheduled.

D. Field Procedures for Abstraction Staff at Data Collection Sources:

1. At data collection sources, keep all ADDM confidential materials in the secure briefcase or computer carrier whenever these materials are not actually being used. Confidential ADDM data or equipment should never be left loose and accessible.
2. Never keep passwords or access phone numbers on the laptop or in the briefcase with the computer. It is recommended that Auto complete for usernames and passwords be disabled.
3. When at the data source, the secure briefcase and project materials must be within sight of the authorized person at all times, in a secure area with password lock enabled, or locked in a secure location without others' access.
4. When you are not directly monitoring your laptop's screen (when reading an evaluation, getting a record while in the same room, etc.), activate the password lock to protect data from visual observation by persons not authorized to work with these materials. During use, laptop screens should be positioned to prevent unauthorized individuals from viewing confidential information.
5. If project materials (including laptop) have to be taken home for any reason, they must be kept in a locked briefcase or computer carrier and stored in a concealed area at all times.
6. CDC requires the use of security cables with all laptops (anytime not in a secure container).
7. Use a virtual private network (VPN) for any remote access for laptops containing confidential information. A VPN is a way to use a public telecommunication infrastructure, such as the internet, to provide remote offices or individual users with secure access to their organization's network.
8. Enable security features on any wireless (Wi-Fi, 802.11) link used for communications.
9. Always turn the computer's Wi-Fi radio and software off when not in use.
10. Use only wireless networks with WPA or WPA2 authentication protocol that requires authentication before granting access. Do not use wireless local area networks (WLANs) configured for public or open access.
11. Rely on trusted sources for web addresses. Adjust internet use in accordance with the risk.

IV. Loss of Project Materials Containing Confidential Data:

1. General Procedures:

a. In the event that any project materials or equipment (laptops, flash drives, etc.) are lost or stolen, contact your supervisor immediately and inform him or her as to whether any materials containing identifying information were included.

b. In the case of theft, contact the local authorities, as appropriate.

c. The site's Principal Investigator (PI) should immediately contact the CDC Project Officer, Victoria Wright, and the CDC Co-Principal Investigators, Jon Baio and Catherine Rice. If you are unable to reach them, please contact the ADDM Project Coordinator, Anita Washington.

d. In the case that identifying information is lost or stolen; the PI should immediately contact those data sources who had identifiable information compromised to work with them in an effort to prevent or minimize potential harm to individuals at risk to having their data compromised.

e. The PI should determine how to handle notification of the disclosure, based on the agreements made with the sources and on the guidelines and regulations of their institutions and state(s).

f. Letters and/or contacts with data sources should include information about the data security procedures that were in place, their implementation, and remediation actions taken by the funded source following the loss or theft.

g. The site PI should keep CDC advised on this matter and be prepared to respond to inquiries regarding this event.

h. If the project materials or equipment are recovered the site will still need to notify those sources that were affected by the theft. There is still the possibility that the information has been compromised.

i. The site PI should provide a written summary to CDC describing the steps taken to resolve the issue.

2. Levels of Information Loss and Consequences:

a. **Unavoidable Loss:** Unavoidable loss of data is defined as loss of data following reasonable steps to protect its security by following these guidelines at a minimum. This type of loss should result in, at a minimum:

- A review of the confidentiality and security agreement with all employees accessing identifying data;
- A record of the incident for the Site's and CDC's files;
- An organizational review of the Site's and ADDM Surveillance Data Confidentiality and Security Agreement.

b. **Loss Due to Negligence:** Loss of data due to project personnel negligence by not following the above-mentioned guidelines should result in, at a minimum:

- Immediate removal of access to identifying or sensitive materials pending review of incident;
- A record of the incident should be placed in the personnel file and forwarded to CDC;
- Additional site-specific personnel procedures may apply and permanent removal from duties can be considered where identifying information is accessible or removal from the ADDM project.

c. **Inappropriate transmission** of data (via email or text messaging) by not following the above-mentioned guidelines should result in, at a minimum:

- Immediate removal of access to identifying or sensitive materials pending review of incident;
- A record of the incident should be placed in the personnel file and forwarded to CDC;
- A review of the confidentiality and security agreement;
- Additional site-specific personnel procedures may apply and permanent removal from duties can be considered where identifying information is accessible or removal from the ADDM project.

d. **Breach by Personnel:** Active divulging of information could be in the form of a verbal disclosure, or in giving unauthorized personnel access to identifying data. Breach of confidentiality due to divulging confidential information by personnel will result in:

- Release from working on the ADDM project;
- Reassignment to another project is at the discretion of each ADDM site in conjunction with site-specific personnel guidelines;
- A record of the incident should be placed in the personnel file and forwarded to CDC.

ADDM Network Data Confidentiality and Security Agreement

A1 Confidentiality Statement of Understanding for ADDM Staff

In accordance with the Privacy Act of 1974 (5 U.S.C. 552a), I, as a personnel member working on a CDC-funded ADDM Surveillance Project, may be given access to personally identifiable data that is covered by the Privacy Act and should be kept strictly confidential and used for project purposes only. As a condition of this access and my participation in this project I am required to comply with the following safeguards as specified in "The ADDM Surveillance Data Confidentiality and Security Agreement" for individuals and establishments against invasions of privacy.

1. I agree to be bound by the following assurance:

   All individuals identified for this project are assured that the confidentiality of their information will be maintained and that no information obtained in the course of this activity will be disclosed by me in a manner in which the individual or establishment is identifiable, unless the individual or establishment has consented to such disclosure, to anyone other than authorized staff of the project.

2. I agree to maintain the following safeguards, at a minimum, to assure that confidentiality is protected and to provide for the physical security of the records:

   To preclude observation of confidential information by persons not authorized to have access to the information on the project, I shall maintain all records from which individuals or establishments could be identified in locked containers or protected computer files when not under immediate supervision by me or another authorized member of the project. The keys or means of access to these containers or files are not to be given to anyone other than authorized staff.

3. I have read, understood, and I further agree to abide by any additional requirements imposed by the *ADDM Data Confidentiality and Security Agreement* for safeguarding the identity of individuals and establishments.

4. I agree that in the event that confidential information is disclosed inadvertently, I will (a) advise the Principal Investigator/Project Coordinator of the incident who will report it to the CDC ADDM Team Lead (Jon Baio) and/or CDC ADDM Co-Principal Investigator (Cathy Rice), (b) safeguard or destroy the information as directed by the investigator, and (c) not inform any other person of the disclosed information.

My signature below indicates that I have carefully read and understand this agreement and the assurance which pertains to the confidential nature of all records to be handled in regard to this project. As a (n) (_____) (principal investigator, abstractor, clinician reviewer, data manager, guest researcher, programmer, etc.), I understand that I am prohibited from disclosing any such confidential information that has been obtained under this project to anyone other than authorized staff of the project. I understand that any disclosure in violation of this Confidentiality Pledge may lead to my removal from working on the ADDM project and additional employment penalties may apply.

Name (printed):_____

Signature: _____ Date: _____

Copy placed in personnel file __

A2 Our Responsibility to Protect Personal Information (HHS – Staff document)

To: HHS-Staff
Subject: Our Responsibility to Protect Personal Information

HHS Colleagues,
As the HHS Chief Information Officer, I want to remind you that we each have the responsibility to protect private information and of actions you should take to keep data secure. You've probably seen reports in the news lately about companies and government agencies "losing" personal, financial, or medical information in a way that puts their employees, customers, patients, or business partners at risk. A stolen laptop, a misplaced backup disk, or a file left on a computer in an internet café - any of these situations could put private information into the wrong hands, leading to the risk of identity theft, credit card theft, or wider publication of personal medical information. And once control of private information has been lost, it's often impossible to get it back.

Any one of us would feel terrible if we were responsible for the loss or theft of confidential or sensitive information that included social security numbers, medical diagnoses, or financial accounts. To put thousands or millions - or even one - person at risk is a terrible burden, and also can result in professional and legal repercussions. Here are a few steps you can take to protect private information:

* Don't keep private information that you don't need to do your job.
Be on the lookout for old report files, backup disks, and spreadsheets on your computer or in your possession that contain personally identifiable information. If you don't need that information to do your job, talk to your supervisor about disposing of the data, records management issues, and data security issues.

* Remove unneeded private information from any laptop or removable storage device.
Laptops and removable storage ("thumb drives," external hard drives, CD-ROMs, etc.) are particularly vulnerable to loss and theft, putting the data stored on them into the wrong hands. Even computer servers and desktop computers in your office and home are susceptible to theft, so removing unneeded private information is a good practice no matter where it's stored.

* Encrypt private data that you must store.
If you must store private information on your desktop computer, on a laptop computer, on a network drive, on removable storage, or on a backup disk, that data must be encrypted in a way that ensure the data won't be usable by an unauthorized person who gains access to it. Encrypting files doesn't need to be complicated. For example, Word, Excel, and WinZip all have encryption capabilities to help protect data, although for full encryption protection, you'll need to use more sophisticated encryption software. Contact your computer support or Computer Information Security Officer for help on this.

* Clear out Web browser sessions.
In general, you should not access private information via a web browser on a publicly accessible computer at a library, hotel, or internet café. If you access private information via a web browser, be sure to "clean up" any temporary files created during your use of that computer. In the course of

any internet session, web browsers like Internet Explorer create temporary files to store the graphics and data that are displayed on your screen. Many of those temporary files can remain on the computer after you've walked away, which can be a problem if you've accessed private information.

To delete temporary files on a Windows computer using Internet Explorer:

-- Click the Tools menu, select Internet Options, and then the General Tab
-- In the Temporary Internet Files box, click the Delete Files button and the checkbox to Delete All Offline Content, and then click OK.
-- In the General Tab section, in the History box, click the Clear History button.
-- Go to the computer's desktop screen, right click the Recycle Bin and select Empty Recycle Bin.

This may seem a bit complicated the first time you go through it, but it only takes a few seconds to delete the data you may have left on that publicly accessible computer, which is important. If you use a different type of browser or computer, talk to your computer support on how to do this.

* Review telework agreements to ensure they address records management and security practices.
Supervisors must ensure that employees who remove data from the office are approved to telework and that the telework agreements appropriately address records management and security practices.

By following these steps, YOU can help ensure that YOU are not the cause of a breach of data security. These are not just "nice to do" actions - they are responsibilities for each of us that are in laws, regulations, and policies and that have penalties for non-compliance. More information can be found in the HHS Policy for IT Security for Remote Access, HHS-IRM-2000-0005 and HHS OCIO Policy for Personal Use of Information Technology Resources, HHS-OCIO-2006-0001, located at http://www.hhs.gov/read/irmpolicy/ , as well as in the HHS Information Security Program Policy, HHS Information Security Program Handbook and HHS Information Security Rules of Behavior, located at http://intranet.hhs.gov/infosec/policies_guides.html.

Each of us are required to report any security incident, or suspected incident, to the applicable Department security office and/or management as soon as possible. If you feel that private information or government equipment has been compromised in any way, report the incident to your supervisor and computer support staff immediately.

Thank you for your efforts and for your attention and action in the important tasks of protecting private information.

Charles Havekost

HHS Chief Information Officer