http://isp-v-maso-apps//policy/Doc/policy385.htm\

Copied from above CDC intranet site 3/16/2011

Category: General Administration
CDC-GA-2005-14 (Formerly CDC-102)
Date of Issue: 04/16/03 Updated: 09/07/05[1][2][3]
Proponent: Office of the Director, Associate Director for Science
Material Superseded: None

CDC/ATSDR Policy on Releasing and Sharing Data[*]

Sections:

I. BACKGROUND

The Centers for Disease Control and Prevention (CDC)[†] and the Agency for Toxic Substances and Disease Registry (ATSDR) are the nation's principal disease prevention and health promotion agencies.[1] To fulfill their missions, these agencies must collect, manage, and interpret scientific data.

CDC believes that public health and scientific advancement are best served when data are released to, or shared with, other public health agencies, academic researchers, and appropriate private researchers in an open, timely, and appropriate way. The interests of the public—which include timely releases of data for further analysis—transcends whatever claim scientists may believe they have to ownership of data acquired or generated using federal funds. Such data are, in fact, owned by the federal government and thus belong to the citizens of the United States.

However, although CDC recognizes the value of releasing data quickly and widely, CDC also recognizes the need to maintain high standards for data quality, the need for procedures that ensure that the privacy of individuals who provide personal information is not jeopardized, and the need to protect information relevant to national security, criminal investigations, or misconduct inquiries and investigations. The goal is to have a policy on data release and sharing that balances the desire to disseminate data as broadly as possible with the need to maintain high standards and protect sensitive information.

This data release/sharing policy will also ensure that CDC is in full compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA),[2] (where applicable) the Freedom of Information Act [FOIA],[3] and the Office of Management and Budget Circular A110,[4] and the Information Quality Guidelines.

II. PURPOSE

The purpose of CDC's data release/sharing policy is to ensure that (1) CDC routinely provides data to its partners for appropriate public health purposes and (2) all data are released and/or shared as soon as feasible without compromising privacy concerns, federal and state confidentiality concerns, proprietary interests, national security interests, or law enforcement activities.

III. DATA COVERED BY THIS POLICY

This policy applies to any new data collection occurring 90 days or more following approval of this policy. Existing (previously established) data collections systems should be in compliance with this policy either within 3 years of policy approval (the cycle for surveillance and information system evaluation stipulated by the CDC Surveillance Coordination Group) or at the time of data system revisions, whichever occurs first. All data should be released as soon as feasible without compromising privacy concerns, federal and state confidentiality concerns, proprietary interests, national security interests, or law enforcement activities. Requests for data during a public health emergency will be handled on a case-by-case basis. The following data are covered by this policy:

- Data collected by CDC using federal resources.
- Data collected for CDC by other agencies or organizations (through procurement mechanisms such as grants, contracts, or cooperative agreements).
- Data reported to CDC (e.g., by a state health department).[5]

For the purpose of this policy, we use the following definitions:

CDC personnel: CDC employees, fellows, visiting scientists, and others (e.g., contractors) who are involved in designing, collecting, analyzing, reporting, or interpreting data for or on behalf of CDC.

Data: Scientific records which are as accurate and complete as possible.

Data release: Dissemination of data either for public use or through an ad hoc request that results in the data steward no longer controlling the data.

Data sharing: Granting certain individuals or organizations access to data that contain individually identifiable information with the understanding that identifiable or potentially identifiable data cannot be re-released further unless a special data sharing agreement governs the use and re-release of the data and is agreed upon by CDC and the data providers.

For a complete list of terms used in this policy, see Appendix B.

IV. DATA NOT COVERED BY THIS POLICY

This policy does ***not*** cover data shared with CDC but owned by other organizations (e.g., data provided to CDC by a managed care organizations, preferred provider organizations, or technology firms for a specific research project). Such data may be covered by other policies or procedures that reflect pertinent laws, regulations, and agreements (such as FOIA).

V. BENEFITS OF RELEASING OR SHARING CDC DATA

- Sharing data with partners involved in collecting, analyzing, or using data will improve (1) the quality of CDC data and (2) the consistency of data across CDC.
- Sharing data will also (1) ensure that CDC scientists, contractors, awardees, and grantees are held accountable for their findings, (2) provide opportunities for study results to be validated, and (3) uncover new areas for research.[6],[7]
- Quality improves when scientists share data with partners and ask for feedback during data collection and analysis.
- Releasing or sharing data can (1) improve public health practitioners' understanding of various research methods, (2) encourage analysts from other disciplines (e.g., economists, social scientists) to examine public health questions, and (3) build trust with outside partners and the public by allowing an open critique of CDC investigations.

- U.S. states and territories have a long-standing history of voluntarily reporting individually identifiable data to CDC on incident conditions or diseases that are of public health importance.[8] Although the electronic exchange and accumulation of data on individual cases promises public health benefits, it also creates a threat to individual privacy. The Council of State and Territorial Epidemiologists asked CDC to develop procedures that balance the need for data protection with the need to share, as broadly as possible, data collected in the interest of public health. Without such a balance, data may need to be withheld from non-CDC researchers solely to protect individual privacy.

VI. GUIDANCE FOR CIOs

In this document, CDC sets forth (1) the guiding principles to be followed when releasing/sharing data and (2) the various ways in which data can be released. Each Center/CDC organization, however, is responsible for developing specific procedures for its staff to follow. Indeed, because issues related to data release can vary from project to project, Centers/CDC organizations may need specific data release procedures for each project. For example, state and local health departments have a continuing ownership and interest in whether and how CDC re-releases data they have supplied. Custodians of such data should consult the CDC-CSTE Intergovernmental Data Release Guidelines Working Group report-

+http://intranet.cdc.gov/od/ocso/ssr/drgwg.pdf which contains data release guidelines and procedures for CDC programs re-releasing state-provided data. The guidelines and procedures in the Working Group report may be useful for other data systems as well."

Guiding Principles

All CDC procedures on releasing or sharing data must be guided by the following principles.

Accountability

As a public health agency of the U.S. government, CDC is accountable to the public and to the public health community for the data it produces through research. By extension, CDC scientists are accountable for their work, and their findings are subject to independent validation. CDC scientists must conduct research with integrity; the resulting data must be of the highest possible quality; and funds must be fully accounted for.

Privacy and confidentiality

CDC recommends that, unless there is a valid public health purpose (e.g., a longitudinal study that requires record linkage), programs should not collect nor maintain identifiable data.

$ **Trust**: Any release or sharing of public health data will acknowledge that (1) data systems are built on trust between the individuals who provide personal data and the agencies that collect those data and (2) that CDC will respect the privacy rights of individuals and others who provide personal or proprietary data. All release/sharing must be consistent with the confidentiality assurances under which the data were collected or obtained.

$ **Privacy Act:** Identifiable data that are maintained in certain systems of records may only be released in accordance with the Privacy Act (http://www4.law.cornell.edu/uscode/5/552a.html) which generally permits disclosing such data only with consent. However, the Privacy Act does permit data release without a subject's consent under limited conditions. One example is a release that is compatible with the purpose for which the data were collected.

$ **Formal confidentiality protection for research subjects:** Some data collected by CDC may be given formal confidentiality protection under

Sections 301(d) or 308(d) of the Public Health Service (PHS) Act. Programs that apply for such protection must make a compelling case that the information sought is so sensitive that research subjects are unlikely to provide valid data without this formal confidentiality protection.[‡] When data have formal confidentiality protection, CDC's policy is to share those data only under conditions that are consistent with the conditions under which the data were collected. It is CDC's responsibility to ensure that inadvertent disclosure does not occur (See Appendix C).

Stewardship

CDC holds data in public trust. Good stewardship of data requires that CDC release or share data in accordance with the objectives and conditions under which the data were collected or obtained and that appropriate policies and procedures for data release be set up.[9]

Scientific practice

Before any data are released/shared, all phases of data collection, transmission, editing, processing, analysis, storage, and dissemination must be evaluated for quality.[10],[11] Preliminary data from a research project may be shared with outside partners for quality assessment but not for publication. Personnel who share data for quality assessment must follow procedures that are consistent with confidentiality agreements and other constraints.

Efficiency

Releasing data to the public and sharing data with partners is an efficient way of ensuring that data are used to their full potential, that work is not duplicated, and that funds are not spent unnecessarily.

Equity

CDC affirms the principles and practices developed to ensure impartiality and credibility of federal statistical activities.[8,][12] CDC strives to have data release policies that are fair to all users, regardless of their organizational affiliation.

VII. HOW TO RELEASE DATA

All released data must be as complete and accurate as possible, and data must be released in accordance with the guiding principles set out in this document in one of two ways:

- Release for public use without restrictions.
- Release to particular parties with restrictions.

Restrictions can be imposed because of legal constraints or because releasing the data would risk (1) disclosing proprietary or confidential information or (2) compromising national security or law enforcement interests.

CDC recommends that data be released in the form that is closest to microdata and that still preserves confidentiality.

Release of data for public use

Data that CDC collects or holds and that can be legally released to the public should be released through a public-use data set within a year after the data are evaluated for quality and shared with any partners in data collection. Procedures for releasing public-use data should be consistent with CDC's Public Health Information Network's functions and specifications.

To ensure that issues of confidentiality, proprietary use, and informed consent are addressed correctly, CIOs may choose to develop specific data release plans for each data set. Each plan should include the following:

- A procedure to ensure that confidential information is not disclosed, for example, a list of steps to reduce this risk.[13],[14]

- A procedure to ensure that data are released in a form that does not endanger national security or compromise law enforcement activities.[15]
- A procedure to ensure that proprietary data (i.e. data owned by private organizations such as Managed Care Organizations, Preferred Provider Organizations, or technology firms) are not released inadvertently.
- Analysis plans and other documentation required by the OMB regulation on data quality.
- Instructions for non-CDC users on the appropriate use of the data.
- The date the data will be released, which should be as soon as possible after they are collected, scrutinized for errors, and validated. This release should occur no more than one year after these activities.
- The formats in which the data will be released (e.g., SAS, ASCII). For each format, give specifications (e.g., variable definitions) and information on standards for transmission.[16]

CIOs may release data without restrictions for public use through the CDC Information Center. Data may also be shared through CDC/ATSDR Scientific Data Repository and its data dissemination portal CDC WONDER (URL: http://wonder.cdc.gov/welcome.html)

. Finally, CIOs may respond to individual requests.

Data shared with restrictions

To the extent possible, CDC recommends sharing data that cannot be released for public use with public health partners. For such restricted data, special data sharing agreements must be developed. Below are two examples of how data can be shared with partners; these methods are not mutually exclusive:

- **Data release under controlled conditions:** Data that cannot be released through a public-use data set or a special-use agreement may be analyzed by appropriate non-CDC researchers at CDC-controlled data centers (e.g., the Data Center established at NCHS; see http://www.cdc.gov/nchs/r&d/rdc.htm for a description). Alternatively, CDC may consider licensing non-CDC researchers to use certain data. Licensing would allow researchers access to identifiable data by extending legal responsibilities to those external researchers.[9] Before making the data available, however, CIOs must evaluate any requests for permission to use their confidential or private data to ensure that the data will be used for an appropriate public health purpose.
- **Data release through a special-use agreement:** Data that cannot be released publicly but that need not always be under CDC's control can be released to appropriate non-CDC researchers through a special-use agreement. Such agreements should be specific about issues related to co-authorship, reviews of findings produced through using the data, reports published about those findings, and the date the data are to be returned. All data sharing agreements should include the following:
  - ✓ Evidence that the party to whom the data are being released need the data for a legitimate public health purpose.
  - ✓ A list of restrictions on the use of the data.
  - ✓ The names of every person who will have access to the data.
  - ✓ Information on any laws pertaining to the agreement.

- ✓ Security procedures that the non-CDC user must follow to protect the data from unauthorized use and the penalties for not following them.
- ✓ A list of restrictions on releasing analytic results.
- ✓ Procedures for returning the data. For an example of a set of procedures, see the CDC and ATSDR policy on data release to departing employees.[17] , [18]
- ✓ Provisions that govern emergency requests for identifiable or otherwise confidential data.

An example of a special-use agreement is in the CDC/CSTE Intergovernmental Data Release Guidelines Working Group Report.[5]

VIII. IMPLEMENTATION OF CDC'S DATA-RELEASE/SHARING POLICY

Each CIO will set up procedures to ensure that CDC's policy on data release/sharing is followed. No later than 1 year after this policy is approved, CIOs should send a report on their procedures to the CDC Associate Director for Science (ADS).

One way a CIO might choose to set up procedures on data release/sharing is to authorize a data-release review board to do so. This board might report to the CIO ADS, and it might include the CIO's Information Resources Manager and stewards of relevant data sets for which the CIO is responsible. Where appropriate, subject-matter experts from the CIO should advise the board on specific data release issues.

Components of CIO procedures on data release/sharing

Each CIO must ensure that the following components are in their procedures for data release and data sharing:

An evaluation of data quality:

Evaluation of data quality must include tests for completeness, validity, reliability, and reproducibility. [11]

An evaluation of the risk of disclosing private or confidential information:

Before releasing/sharing any data, the data steward must assess the risk that personal information will be disclosed and decide whether some data need to be further de-identified.[19] For example, under the Health Insurance Portability and Accountability Act (HIPAA), 18 variables are considered identifiers, the removal of which would render the dataset de-identified. This rule, while not applicable to CDC releasing public health information, serves as a useful guide for creating de-identified data and information.[2]

Those assessing the risk that confidential information will be disclosed should recommend the statistical methods to be used for disclosure protection (e.g., suppression, random perturbations, recoding, top- or bottom-coding).[20], [21] The recommended methods should balance the risk of disclosure against the possibility that reducing the risk of disclosure will also reduce the usefulness of the data for public health practice and research.

Documentation:

All released data must have documentation that shows the conditions under which the data were collected, what the data represent, the extent of the data's completeness and accuracy, and any potential limitations on their use. Careful documentation increases the likelihood that secondary data users will interpret data correctly.

Data elements to be documented are listed in Appendix D.

CDC will develop standards for the elements needed to document data. These standards could be developed on the basis of a review of best practices for data archiving.[22],[23] Specifically, CDC standards for documentation should be compatible with those of private industry. For examples of standards, see www.pueblo.lbl.gov; www.fgdc.gov/standards;

www.nbii.gov/datainfo/metadata/standards; www.isotc211.org; http://www.icpsr.umich.edu/DDI; or gcmd.gsfc.nasa.gov/Aboutus/standards.

Public release disclosure statement:

Information that will preclude misinterpretation of data should accompany all released data.

Obligations of non-CDC data users

Public use data agreements should include instructions that non-CDC data users must agree not to link data with other data sets. In addition, these agreements should include instructions to report to the CDC ADS any inadvertent discovery of the identity of any person and to make no use of that discovery.

Obligations of grantees, contractors, and partners

As of three years following approval of this policy, CDC expects researchers who are supported by CDC funding to make their data available for analysis by other public health researchers. Consequently, CDC requires that mechanisms for, and costs of, data sharing be included in contracts, cooperative agreements, and applications for grants. CDC reviewers must check whether applications for CDC funds include mechanisms for, and costs of, sharing data. The costs of sharing or archiving data may be included in the amount of funds requested in applications for first-time or continuation funds. Applicants for CDC funds who incorporate data release into their study designs can (1) readily and economically set up procedures for protecting the identities of research subjects and (2) produce useful data with appropriate documentation. Awardees who fail to release data in a timely fashion will be subject to procedures normally used to address lack of performance (e.g., reduction in funding, restriction of funds, or grant termination).[24] Researchers who contend that the data they collect or produce are not appropriate for release must justify that contention in their applications for CDC funds.

IX. MEMORANDA OF UNDERSTANDING (MOUs) ALREADY IN PLACE

CIOs should examine the MOUs they have with other organizations or agencies to ensure that they are consistent with this data release and sharing policy and with any program-specific implementations of this policy. New MOUs should be written to ensure consistency with this policy. Any CIOs with MOUs that are inconsistent with CDC's data release policies should report that fact to the CDC ADS. Include in the report information about whatever steps have been taken to bring the MOUs into compliance with CDC's data release/sharing policy.

X. TRAINING

To ensure that this policy is followed correctly, CIOs must train their personnel in the procedures for data release/sharing. They can do so in several ways: through new Human Resources Management Office (HRMO) courses, during new employee orientation programs, at ethics certification courses, or as part of training on the CIO's local area network (LAN).

XI. CDC's COMMITMENT

CDC is committed to establishing and implementing procedures based on this policy. In addition, CDC will swiftly address any breach in the policy. Breaches consist of willful acts (e.g., deliberate disclosures that constitute scientific misconduct as defined by the Office of Research Integrity) and inadvertent disclosures (e.g., errors in judgment with no intent to do harm).

Appendix A: Committee members (listed alphabetically)[§]

Representative	**CIO**	**Other Representation**
Coleen Boyle, PhD	NCCDPHP	Excellence in Science Committee
Susan Chu, PhD, MSPH	NIP	Vaccine Safety Data Link Project
Betsey Dunaway, MS, EdS.	MASO	Confidentiality Protections, Privacy Act
David Elswick	EPO	CDC Managed Care Task Order
Jeanne Gilliland	NCCDPHP	CDC Information Council
Ruth Ann Jajosky, DMD, MPH	EPO	CDC-CSTE Intergovernmental Data Release Guidelines Working Group
Paula Kocher	OD/OGC	Deputy Legal Advisor
Jennifer Madans, PhD	NCHS	DHHS Data Quality Committee
Catherine Spruill	OD	Office of CDC ADS
Norm Staehling	NCEH	
Donna F. Stroup, PhD, MSc	NCCDPHP	Excellence in Science Committee, Chair Working Group
Wendy Watkins	OD	Office of CDC ADS

G. David Williamson, PhD ATSDR Federal Committee on Statistical Methodology

Appendix B: Glossary

Archiving data	Storage of data for secondary use, with or without an expiration date and with or without the informed consent of those who provided private or confidential information.
Confidentiality	The treatment of information entrusted to CDC with the expectation that it will not be divulged to others in ways that are inconsistent with the conditions agreed to when the information was originally disclosed**.**
Controlled access	A system that allows researchers restricted use of data that cannot be released either to the public or under special use agreements. Researchers can use the data but cannot have possession.
Data	Scientific records which are as accurate and complete as possible.
Data release	Dissemination of data either for public use or through an ad hoc request that results in the data steward no longer controlling the data. This does not include the release of data under FOIA.
Data sharing	Granting certain individuals or organizations access to data that contain individually identifiable information with the understanding that identifiable or potentially identifiable data cannot be re-released further unless a special data sharing agreement governs the use and re-release of the data and is agreed upon by CDC and the data providers.
Data steward	The CDC employee responsible for explaining CDC's data policy to staff and users, developing and maintaining data systems, evaluating and approving requests for access to data, and monitoring compliance with CDC policy.
Disclosure control	Procedures used to limit the risk that information about an individual will be disclosed. These procedures may be administrative (e.g., granting authorized access), physical (e.g., setting up passwords), or statistical (e.g., cell suppression, aggregation, perturbation, and top- or bottom-coding). Usually statistical procedures are followed when preparing a public-use data set or a data set that is linkable to another released data set.

Identifiable data	Data which can be used to establish individual identity, either "directly," using items such as name, address, or unique identifying number, or "indirectly" by linking data about a case-individual with other information that uniquely identifies them.
Microdata	Data files or records on an individual person or facility
Privacy rights	The right of people to hold information about themselves free from the knowledge of others.[25]
Proprietary	Produced or collected in such a way that exclusive rights may apply.
Public health emergency	The occurrence or imminent threat of an adverse health event caused by epidemic or pandemic disease, infectious agent, biologic or chemical toxin, environmental disaster, or any agent that poses a real and substantial risk for a significant number of human fatalities or cases of permanent or long-term disability.
Public-use data	Data available to anyone.
Restricted data	Data that are shared only in a limited way because greater dissemination could have a negative effect, for example on national security.
Security	Any mechanisms (administrative, technical, or physical) by which privacy and confidentiality policies are set up in computer or telecommunications systems.

Appendix C: Applicable Laws and Rules

Receiving Data at CDC

I. Health Insurance Portability and Accountability Act
P.L. 104-191
Privacy Rule - 45 CFR
Parts 160 and 164
http://cms.hhs.gov/hipaa/hipaa1/default.asp

II. Federal Educational Rights and Privacy Act (FERPA)
20 USC 1232(g)
http://www.ed.gov/offices/OM/fpco/ferpa/index.html

Releasing Data from CDC

I. National Security
Freedom of Information Act (FOIA)
5 USC § 552
45 CFR § 5.62
http://www.usdoj.gov/oip/exemption1.htm

II. Proprietary Data
1) FOIA Exemption 4
45 CFR § 5.65
http://www.usdoj.gov/oip/exemption4..htm
2) Trade Secrets Act
18 USC § 1905

III. Predecisional
FOIA Exemption 5
45 CFR § 5.66
http://www.usdoj.gov/oip/exemption5.htm

IV. Privacy
1) Human subjects common rule
45 CFR § 46
http://ohrp.osophs.dhhs.gov/humansubjects/guidance/45cfr46.htm
2) FOIA Exemption 6
45 CFR § 5.67
http://www.usdoj.gov/oip/exemption6.htm
3) Assurances/Certificates of Confidentiality
Sections 301(d) & 308(d) of the
Public Health Service Act
42 USC 241(d) & 42 USC 242 (m)(d)
http://www.fda.gov/opacom/laws/phsvcact/phsvcact.htm
4) Privacy Act
5 USC § 552a; 45 CFR § 5b
http://www4.law.cornell.edu/uscode/5/552a.html
http://www2.ihs.gov/Privacy Act/regulations/index.asp

V. Law Enforcement
FOIA Exemption 7
45 CFR § 5.68
http://www.usdoj.gov/oip/exemption7.htm

VI Information Quality Guidelines
http://www.hhs.gov/infoquality
http://www.hhs.gov/infoquality/cdc.html

Appendix D: Recommended Data Documentation Elements

1) Name of person responsible for the data or the person to contact about using the data.
2) Overview on the data:
   a) Description of the original project.
   b) Source of the data.
   c) Background information on the study design.
   d) Information about data collection activities and data collection instruments used (e.g., a questionnaire).
   e) Information about how the data were processed, including how missing values were handled.
   f) Information on the filters applied to the data.
   g) Statistical and analytical procedures used on the data.

3) Period covered by the data.

4) Date and place of publication of the data.

5) If the data were modified after publication, date such a modification occurred.

6) A data dictionary that describes the variables, data values, and coding classifications for the variables used in the original data set and for those derived from the original variables (e.g., constructed variables), including geographic codes and weighting variables, if any.

7) A complete list of the data files that make up the data set.

8) The confidentiality procedures applied to the data (e.g., cell suppression, record omission) in order to limit the potential for re-identification.

9) Precalculated tables or frequency counts that act as control tables for validating that the data are read correctly.

10) Information on any constraints on data access or data use; include information on any data-use agreements.

11) Any other information data users need, including information on caveats or limitations about the data.

12) Format in which the data are available (e.g., ASCII, DBF).

13) Medium in which the data are stored (e.g., CD-ROM, Internet).

XII. References

[*] The names of committee members who produced this document are listed in Appendix A.
[†] Throughout this document, *CDC* should be understood to refer to CDC and ATSDR.

[‡] Section 308(d) protects all NCHS survey data by way of legislative authority.
[§] The committee thanks Helen McClintock for her excellent editing of this document and Kenya S. Ford for her legal review.

1. Centers for Disease Control and Prevention. Available at: URL: http://www.cdc.gov. accessed September 23, 2002.

2. Health Insurance Portability and Accountability Act of 1996 (HIPAA) . Available at URL: http://cms.hhs.gov/hipaa/hippa/default.asp . Accessed September 23, 2002.

3. Freedom of Information Act (FOIA)-Title 5 USC 552. Available at URL: http://www4.law.cornell.edu/uscode/5/552.html .

4. Office of Management and Budget (OMB). Uniform administrative requirements for grants and agreements with institutions of higher education, hospitals, and other non-profit organizations. 64 Fed.Reg. 54926 (October 8, 1999), incorporated into 45 C.F.R. Part 74.36 (OMB Circular A-110).
Available at: URL: http://www.whitehouse.gov/omb/circulars/a110/a110.html accessed September 23, 2002.

5. CDC-CSTE Intergovernmental Data Release Guidelines Working Group Report. CDC-ATSDR- Data Release Guidelines and Procedures for Re-release of State-Provided Data. January, 2005. Available at URL: http://www.cdc.gov/od/foia/policies/drgwg.pdf

6. Campbell EG, Clarridge BR, Gokhale M, Birenbaum L. Hilartner S, Holtzman NA, Blumenthal D. Data withholding in academic genetics: evidence from a national survey. JAMA 2002;287:473-80.

7. Koo D, Wetterhall SF. History and current status of the National Notifiable Diseases Surveillance System. J Public Health Management Practice. 1996;2(4):4-10.

8. Committee on National Statistics, Commission on Behavioral and Social Sciences and Education. National Research Council. Martin ME, Strat ML, Citro CF. Principles and practices of a federal statistical agency 2nd ed. Washington: National Academy Press; 2001. Available at: URL: http://www.nap.edu/ Accessed September 23, 2002.

9. Doyle P, Lane J, Theeuwes H, Zayatz L, editors. Confidentiality, disclosure, and data access: theory and practical application for statistical agencies. Amsterdam: Elsevier; 2001. Available at: URL: http://www.census.gov/srd/sdc. Accessed September 23, 2002.

10. Office of Management and Budget. Guidelines for ensuring and maximizing the quality, objectivity, utility, and integrity of information disseminated by federal agencies. Federal Register 2002:2:67;369-78. Available at: URL: http://www.whitehouse.gov/omb/fedreg/reproducible.html. Accessed September 23, 2002.

11. Department of Health and Human Services. Draft guidelines for ensuring and maximizing the quality of information disseminated to the public, May 1, 2002. Available at URL: <http://www.hhs.gov/infoquality/cdc.html>. Accessed September 23, 2002.

12. Federal Committee on Statistical Methodology. Report on statistical disclosure methodology (statistical working paper 22). Washington: Office of Management and Budget, Office of Information and Regulatory Affairs, Statistical Policy Office: May 1994. Available at: URL: http://www.fcsm.gov/working-papers/wp22.html. Accessed September 23, 2002.

13. Interagency Confidentiality and Data Access Committee, Federal Committee on Statistical Methodology Checklist on disclosure potential of proposed data releases. Washington: Office of Management and Budget, Office of Information and Regulatory Affairs, Statistical Policy Office; 1999 www.fcsm/gov/CDAC/index.html .

14. National Center for Health Statistics (NCHS), CDC. NCHS Policy on Micro-Data Dissemination. July 2002.

15. Executive Order 12958 (CDC-IR-2002-03: Information Resources Management—Policy on Classified Material, rev 2002. Available at: URL: http://intraspn.cdc.gov/maso/policy/Doc/policy302.htm HHS authority 46 F.R. 239 (2001)).

16. CDC Information Council. Available at: URL: www.cdc.gov/cic. Accessed September 23, 2002.

17. CDC-GA-2005-06, Clearance of Information Products Disseminated Outside CDC for Public Use. Available at: URL: http://intraspn.cdc.gov/maso/policy/Doc/policy66.htm Updated July 22, 2005.http://intranet.cdc.gov/maso/isso/itaccess.htm

18. CDC-IR-2000-01, Record Keeping Procedures for Managing e-mails and Attachments that Qualify as Federal Records. Available at: URL: http://intraspn.cdc.gov/maso/policy/Doc/policy238.htm Accessed September 23, 2002.http://intranet.cdc.gov/maso/isso/itaccess.htm

19. O'Brien DG, Yasnoff WA. Privacy, confidentiality, and security in information systems of state health agencies. Am J Prev Med 1999;16(4):351-8.

20. Federal Committee on Statistical Methodology. Report on statistical disclosure methodology [statistical working paper 22]. Washington: Office of Management and Budget, Office of Information and Regulatory Affairs, Statistical Policy Office; May 1994. Available at: URL: http://www.fcsm.gov/working-papers/wp22.html. Accessed September 23, 2002.

21. Klein RJ, Proctor SE, Boudreault MA, Turczyn KM. Healthy People 2010 Criteria for Data Suppression. Statistical Notes, no. 24. Hyattsville, Maryland: National Center for Health Statistics, CDC. July 2002. Available at: URL : http://www.cdc.gov/nchs/data/statnt/statnt24.pdf Accessed September 23, 2002.

22. University of Essex. United Kingdom Data Archive. Good Practice in Data documentation. Essex Available at: URL: http://www.data-archive.ac.uk/creatingData/goodPractice.doc. Accessed September 23, 2002.

23. Rockwell RC, Abeles RP. Sharing and archiving data is fundamental to scientific progress. J Gerontol B Psychol Sci Soc Sci 1998;53(1):S5-8.

24. Federal Acquisition Regulations, Subpart52.227-14, Rights in data. Available at: URL: http://www.arnet.gov/far/. Accessed September 23, 2002.

[1] Revised text in Section VI to refer to CDC-CSTE Intergovernmental Data Release Guidelines Working Group Report.
[2] Revised Reference 5 to refer to final report of *CDC/ATSDR Data Release Guidelines and Procedures for Re-release of State-Provided Data*, issued January 2005.
[3] Revised Section VII to reflect current CDC organization regarding CDC/ATSDR Scientific Data Repository data dissemination portal CDC WONDER.