It is necessary to remember FOI requests do not include requests for records which are normally prepared for public distribution, such as press releases, fact sheets, information brochures, speeches, etc. Such records will be provided promptly to any requester without reference to the FOIA, without referral to an FOI staff, and without collecting any fees.

6. THE PHYSICAL PROTECTION OF RECORDS

Employees of CDC are responsible for protecting all confidential records—from eye observation, from theft, or from accidental loss or misplacement due to carelessness.

On this subject the Privacy Act prescribes (Section 552a(e)) 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 . . . .

Absolute protection of the records would be impossible; nevertheless, all reasonable precautions (i.e., all that staff could reasonably be expected to do) must be taken to protect them.

6.1 Policy

It is policy of CDC that to insure the confidentiality of records the following steps are observed:

A. Confidential records must be kept locked up at all times when they are not actually being used. That is, they must be kept in locked fireproof cabinets or in locked rooms after business hours and whenever the persons using them are not present. Only a limited number of staff, as authorized by the Center/Institute/Office Director, may have keys or other means of access to such cabinets or rooms.
B. When confidential records are in use, 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 are not to be made. Any duplicate copies made of confidential records are to be destroyed as soon as operational requirements permit.
D. When records are transferred to archives or 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 CDC.
E. When CDC confidential records are in the possession of other agents of CDC, their protection must be guaranteed by contract provision subscribed to and signed by the agent. The contractor must also be made liable to legal sanctions if the confidentiality pledge should be violated.
F. In all epidemiological or statistical programs of CDC involving confidential information, records containing identifiers of individuals or establishments should be held to the minimum number deemed essential to perform CDC's functions. Identifiers are never to be carried beyond the original survey or report document when the data are processed, unless there is a legitimate and important reason for doing so. Moreover, the documents containing identifiers are to be sent to storage as soon as it is feasible to do so.

7. AUTHORIZED DISCLOSURES

7.1 Disclosure to the Parent Locator Service

With but one exception, *no* information about a person or establishment may be disclosed to anyone without the informed consent of the person or establishment supplying the information or described in it. That single exception is contained in the 1974 Amendments to the Social Security Act relating to the Parent Locator Service (42 U.S.C. 653) which reads in part:

> (b) Upon request, filed in accordance with Subsection (d), of any authorized person (as defined in Subsection (c)) for the most recent address and place of employment of any absent parent, the Secretary shall, *notwithstanding any other provision of law*, provide through the Parent Locator Service such information to such person, if such information—(1) is contained in

any files or records maintained by the Secretary or by the Department of Health and Human Services . . . . (Italics added.)

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

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

Under Section 308(d), CDC is permitted to release data for identifiable individual persons or establishments if (1) such release is included in the purpose for which the data were supplied and (2) the particular person or establishment supplying the information or described in it has consented to such release.

If the information to be released relates to one or more identified individuals, then the requirements for disclosures contained in the Privacy Act of 1974 would also have to be met. Such disclosures would, nevertheless, be a departure from common CDC practices on confidentiality; it is not expected that any situations will arise in which CDC will wish to disclose identifiable data on individuals.

7.3 Disclosures Within the Department

The Privacy Act of 1974 considers HHS in its entirety as one "agency," and it permits the disclosure of records "to those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties" (Section 552a(b)(1)). The Department also permits identified data in CDC to be transferred to other parts of the Department when such transfer is included in the purpose for which the data were supplied to CDC. However, CDC would not countenance the transfer of any confidential data obtained under the 304 and 306 provision to another part of the Department without positive assurance that the data will be used only for the authorized purpose and that the confidentiality of the 304 and 306 data will be protected quite as effectively in the other organization as it would be by CDC itself. In any event, no identifiable data may be transferred from CDC to any other part of the Department without the written approval of the Director, CDC.

7.4 Transfers of Data to Other Departments of the Federal Government

Section 3510 of the Paperwork Reduction Act of 1980 provides:

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

(b) If information obtained by an agency is released by that agency to another agency, all the provisions of law (including penalties which relate to the unlawful disclosure of information) apply to the officers and employees of the agency to which information is released to the same extent and in the same manner as the provisions apply to the officers and employees of the agency which originally obtained the information. The officers and employees of the agency to which information is released, in addition, shall be subject to the same provisions of law, including penalties, relating to the unlawful disclosure of information as if the information had been collected directly by that agency.

If an organizational element receives data collected under a legal assurance of confidentiality, please notify OPPE/CDC so that this information can be included in the Repository of Assurances and the appropriate offices notified. This refers only to data made available from another Federal agency.

7.5 Cooperative Arrangements

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

A. Contractual arrangements exist in which another organization either (1) provides a service—such as field collection or keypunching—to CDC or (2) undertakes analysis of data provided by CDC and, in either case, has access and de facto control of microdata. (See Appendix A on confidentiality requirements in data collection contracts and Appendix B for requirements relating to data processing contracts.)

B. In some instances CDC acts formally as "collecting agent" for another Federal agency under conditions specified in a reimbursable agreement.

C. A situation prevails in the morbidity and surveillance area where the State is the collector under its own law. CDC uses the data under an arrangement with the State and abides by the terms of the arrangement.

7.6 Governing Principles

Whatever specific procedures or legal arguments are employed to bring about authorized disclosure of epidemiological and statistical data, CDC action is governed or constrained by three principles:

A. The action leading to disclosure must be clearly within the relevant laws and regulations, and if there is any doubt, the doubt must be resolved by legal counsel.
B. CDC must always be *candid* with respondents, making it clear who will have access to individual responses and for what (general) purpose the data are being collected.
C. An essential requirement for release of data is the *consent* of the respondent.

8. AUTOMATIC DATA PROCESSING SYSTEMS SECURITY

8.1 General

To achieve the goal of security for Federal automatic data processing systems, policy directives have established requirements for the development of management controls to safeguard personal, proprietary, and other sensitive data in these systems. HHS and PHS computer security programs are established to reduce to the lowest acceptable level the risk of loss and unauthorized use of such data. Likewise, the CDC Security Management Plan sets forth a program to institute procedures, techniques, and methodologies for the protection of ADP resources. The program requires the development of physical, administrative, and technical safeguards to adequately protect automated records and ADP equipment.

The ADP security program is intended to provide protections for a number of systems, including but not limited to:

1. Systems applications and data bases whose data have been legislated to a state of confidentiality.
2. Systems in which there is potential for defrauding the Government.
3. Automated systems of records subject to the Privacy Act of 1974.
4. Systems which are the principal sources of information relative to decisions for allocating resources.

The functional responsibility for ensuring adequate safeguards rests with the ADP application systems managers and facility managers of computer,

mini/micro, remote ADP work stations, ancillary facilities, telecommunication services, and contracts which provide ADP support or utilize Government-owned ADP equipment and data. However, others who access or control the data share responsibility for security, including the ADP Systems Security Officer, systems programmers, analysts, computer programmer operators, tape librarians, clerks, and ADP system users.

8.2 Physical Security

Physical security measures consist of conventional door locks as well as card access control equipment at the main entrance to the facility and to the computer room. Requesters must demonstrate a work-related need to enter secure areas before being granted access.

8.3 Data Security

Procedural safeguards include the following:

1. User registration (requires supervisory approval).
2. User cancellation and accountability transfer when the employee transfers within the agency or terminates employment.
3. Assignment of individual user identification codes and organizational account codes.
4. Programmed verification of valid user identification code, valid account code, and valid combination of the two prior to allowing a terminal session or job submission.
5. Assignment of an individual password which must be used in addition to user identification and account code when accessing the system from an ADP terminal.
6. Programmed verification of the user password prior to acceptance of a user terminal session.
7. Daily backup of online data sets to provide for data recovery.
8. Capability for users to employ data set passwords for magnetic tape files.
9. Data Base Management System which provides for password protection of data sets, individual data elements, and update authorization.
10. Individual program libraries on ROSCOE system which allow the user to restrict access to individual members.
11. Overwrite protection for expired data sets to avoid accidental disclosure.
12. Source documents are locked in a metal cabinet inside a locked room during nonduty hours.
13. Release of reports which contain sensitive and/or confidential data requires appropriate signature on inventory records.
14. Storage of data in an offsite, fire-resistant safe.

8.4 Reference

All users of ADP equipment receive instructions concerning the requirements of ADP Systems Manual, Part 6, ADP Systems Security, July 2, 1982.

---

9. AVOIDING INADVERTENT DISCLOSURES IN PUBLISHED DATA

9.1 Problem

In their zeal to make available to the public a full set of information on a given subject, epidemiologists or statisticians may—and sometimes do—present so much detail in published tabulations that they accidentally reveal confidential information about particular study subjects. This may happen in several ways:

A. One line y_i of a cross-tabulation contains a total of two individuals. On reading the table an individual with the y_i characteristic now knows the x characteristic of the other individual in the population having the y_i characteristic.

B. All cases in line y_i of a statistical table fall in the cell in column x_i. We then know that any individual in the population with characteristic y_i also has characteristic x_i.

C. Cell x_iy_i gives the total income of all individuals with characteristics x_i and y_i. If there are only two individuals, *a* and *b*, in the population with that combination of characteristics, then *a*, knowing his own income, will be able to determine *b's* income by simple subtraction, and *b* will also be able to determine *a's* income.

D. A table gives the total annual receipts for all five nursing homes in county *m*. However, nursing home *a* is much larger than all the rest combined; it accounts, in fact, for three-fourths of all nursing home receipts in the county. Knowing the county total, the manager of nursing home *a* is able to calculate the incomes of the other four homes, at least within some fairly narrow limits.

E. A Standard Metropolitan Statistical Area (SMSA) contains two counties, *a* and *b*. Four hospitals are located in county *a* and only one in county *b*. A statistical report is published, giving confidential hospital data totaled for each SMSA. Another report is published with confidential data on hospitals by county, but only for counties with three or more hospitals. Using the two reports one can subtract the data for county *a* from the SMSA data, deriving the confidential data for the lone hospital in county *b*.

F. The maximum Social Security benefit for an individual retired person is, say, $235 per month. A published table shows that white males aged 70 to 74 in county *a* receive an average benefit of $235 per month. It is now known that *every* white male aged 70 to 74 in county *a* who receives a Social Security payment receives $235 a month.

These examples imply the existence of several general types of situations in which statistical disclosure may occur. An additional possibility may be found in a group of three or more tables of subsets of a given population from which disclosures are possible through the solution of simultaneous equations. CDC guidelines as set forth in Section 9.3 take into account the several possible disclosure situations.

9.2 Types of Disclosure

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

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

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

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

9.3 Special Guidelines for Avoiding Disclosure

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

A. In no table should all cases of any line or column be found in a single cell.
B. In no case should the total figure for a line or column of a cross-tabulation be less than three.
C. In no case should a quantity figure be based upon fewer than three cases.
D. In no case should a quantity figure be published if one case contributes more than 60 percent of the amount.
E. In no case should data on an identifiable case, nor any of the kinds of data listed in preceding items A-D, be derivable through subtraction or other calculation from the combination of tables published on a given study.
F. Data published by CDC should never permit disclosure when used in combination with other known data.

Report writers and editors in CDC are to follow these guidelines. If a guideline appears unreasonable in a given situation, approval for a special exception to the guideline should be requested from the Director, CDC. The following types of cases represent exceptions to the above guidelines which do not require special approval from the Director, CDC:

A. It has been a longstanding tradition in the field of morbidity or mortality statistics not to suppress small frequency cells in the tabulation and presentation of data. For example, it has been considered important to know that there were two deaths from rabies in Rio Arriba County, N. Mex., in a given year, or that there were only one infant death and two fetal deaths in Aitkin County, Minn. These types of exceptions to general CDC practices in other programs are followed because they have been accepted traditionally and because they rarely, if ever, reveal any information about individuals that is not known socially.
B. Tables may show simple *counts* of number of persons, even though the number in a cell is only "1" or "2," provided the classifying data are not judged to be sensitive in the context of the table. For example, publication of counts of health manpower personnel by occupation by area are considered acceptable, if not accompanied by other distinguishing characteristics, or other cross-classifications that have the effect of adding descriptive information about the same persons. However, publication of counts of personnel for a specified occupation by area by income is not acceptable for cells of less than three persons because that would reveal sensitive income data.

9.4 Evaluating a Disclosure Problem

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

A. When data in a study are based upon a small-fraction sample, for example, less than 10 percent of the universe, it might generally be assumed that disclosure will not occur through published tabulations. However, there could be exceptions. So much detail may be presented that an individual unique in the population is identified through the tables, or a member of the sample may find himself and others in the data. The usual rules precluding publication of sample estimates that do not have a reasonably small relative sampling error should prevent any disclosures from occurring in tabulations from sample data.
B. The existence of errors or imputations in the data brings some small reduction in the likelihood of disclosure through table publication.
C. Incompleteness of reporting, which often occurs even where studies are supposed to include 100 percent of a given group in the population, also reduces the certainty of any disclosure taking place through publication of data.
D. In some instances, the danger of disclosure might be mitigated by the fact that the data in question have no sensitivity. They may already have appeared in a published directory, or they may involve entirely obvious characteristics; or they may relate to an earlier time. Since that time, many changes have occurred, so that the data have become completely innocuous.

9.5 Measures to Avoid Disclosure

Two methods customarily used in CDC to prevent disclosures from taking place through tabulations:

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