Confidentiality of Research and Statistical Data

Enforcement Assistance Administration
Department of Justice

Confidentiality of Research and Statistical Data

Law Enforcement Assistance Administration
U.S. Department of Justice

U.S. Department of Justice
Law Enforcement Assistance Administration
National Criminal Justice Information and Statistics Service

James M. H. Gregg
Acting Administrator

Harry Bratt
Assistant Administrator
National Criminal Justice Information and Statistics Service

Carol G. Kaplan, Director
Privacy and Security Staff

Preface

This document was prepared by the Privacy and Security Staff, National Criminal Justice Information and Statistics Service, in conjunction with the LEAA Office of General Counsel, to explain and discuss the requirements of the LEAA regulations governing confidentiality of research and statistical data (28 CFR Part 22). It is hoped that the document will clarify some of the requirements and objectives of the regulations and will serve as a guide to persons conducting research and statistical activities pursuant to LEAA-funded projects. Of equal importance, it is hoped that the document will provide potential project subjects with an easily understood statement of the scope and protections of the regulations.

Background

The Statute

The LEAA regulations on confidentiality of research and statistical data, which are contained in 28 CFR Part 22, implement Section 524(a) of the Omnibus Crime Control and Safe Streets Act of 1968, as amended. Section 524(a) provides that:

> Except as provided by Federal law other than this title, no officer or employee of the Federal Government, nor any recipient of assistance under the provisions of this title, shall use or reveal any research or statistical information furnished under this title by any person and identifiable to any specific private person for any purpose other than the purpose for which it was obtained in accordance with the title. Copies of such information shall be immune from legal process, and shall not, without the consent of the person furnishing such information, be admitted as evidence or used for any purpose in any action, suit, or other judicial or administrative proceedings.

The section was enacted as part of the 1973 amendment to the Omnibus Crime Control and Safe Streets Act.

The Regulations

In recognition of the significance of the issues involved, draft regulations implementing the act were initially published in the *Federal Register* on September 24, 1975. Public hearings were conducted on October 11, 1975; written comments were also received from interested groups. Subsequently, on January 8, 1976, an ad hoc panel of interested persons was convened to discuss proposed revisions to the draft regulations. The panel included representatives of the criminal justice, academic, and research communities, as well as representatives of other interested Federal agencies. On December 15, 1976, final regulations were promulgated in the *Federal Register*.

Objectives

The objectives of these regulations are:

(1) to ensure the confidentiality of identifiable data collected for a research/statistical purpose;

(2) to upgrade the validity of research findings (by minimizing subject concern over subsequent use of personal information); and

(3) to clarify researchers' obligations, responsibilities, and protections with respect to use and revelation of identifiable research/statistical data.

Impact

Summary of Requirements

In summary, the regulations provide:

- o that identifiable research/statistical data may only be used (without consent of the individual) for research or statistical purposes;
- o that data may only be transferred in identifiable form pursuant to a transfer agreement ensuring recipient compliance with confidentiality limitations;
- o that, except in noted circumstances, subjects must be advised that data will only be used for research or statistical purposes;
- o that, upon completion of a project, identifiers must be destroyed or otherwise separated from data and permanently secured; and
- o that copies of identifiable data are immune from administrative or judicial process.

Protection to Subjects

The regulations are intended to ensure that information provided for research/statistical use:

- o is not transferred or revealed in identifiable form for any purpose other than additional research or statistical activity (without prior consent of the individual);
- o is not used for purposes other than research/statistical activity (without prior consent of the individual);
- o is not included in identifiable form in reports or publications (without prior consent of the individual); and
- o is maintained under physically and administratively secure conditions to protect against unintentional revelation of identifiable data.

The immunity sections of the regulations ensure that copies of information identifiable to a private person collected for research/statistical purposes cannot be subpoenaed or otherwise legally compelled to be produced in a judicial or administrative proceeding.

Key Concepts

The major areas to be considered in understanding the requirements of the regulations are grouped under the following general subject headings:

Applicability

Information Protected

Information Not Protected

Authorized Uses and Transfers of Data

Subject Notification Requirements

Final Disposition of Data

Security of Data

Immunity

Applicability

The regulations *apply* to all projects that:

- were funded with LEAA funds awarded subsequent to January 14, 1977; and
- involve the collection of information identifiable to a private person for research/statistical purposes.

Coverage extends to research or evaluative "components" of LEAA-funded "action or delivery" projects in cases where identifiable data is collected in the evaluation or research component.

The regulations *do not apply* to:

- projects in which data are collected for a research or statistical purpose in unidentifiable form;
- "action" projects in which identifiable data are collected for administrative or operational uses;
- projects where funds are used for development of data-collection capability--rather than collection of data.

Statutory requirements, including the immunity provisions, apply to all personally identifiable research/statistical data collected in LEAA projects funded after July 1, 1973.

On October 3, 1977, Public Law 95-115 incorporated Section 524(a) into the Juvenile Justice and Delinquency Prevention Act of 1974. Research and statistical projects funded under this Act are now fully subject to the Section 524(a) confidentiality provisions.

Information Protected

The statutory language on which the regulations are based provides that the protections of the statute apply to *research and statistical information* that is *identifiable* to any *specific private person*. The protections apply regardless of the nature, subject matter, or "privacy implications" of the information.

Research and statistical information is defined by the regulations as: "information obtained for a research or statistical purpose in a project (or project component) whose objective is to test, measure, evaluate, or otherwise increase knowledge in a given substantive area."

Under this definition:

- Identifiable information obtained for administrative or "housekeeping" purposes is *not* protected--even where obtained in connection with conduct of a research/statistical project.

- Identifiable information obtained for research/statistical purposes in a component of an otherwise "action/ delivery" program *is* protected under the regulations.

Private person is defined by the regulations as including corporations or nongovernmental organizations, as well as individual persons. The term includes persons (such as law enforcement officials) operating in an official capacity, but excludes governmental agencies.

Under this definition:

- Information identifiable to a law enforcement officer whose activities were the subject of a research or statistical effort *would* be confidential under the regulations.

- Information identifiable to a particular police department *would not* be confidential under the regulations.

Identifiable information is defined by the Regulations as information which may "reasonably" be identified to a private person. The term is to be construed on the basis of factors such as:

- the size of the statistical universe;

- the availability of public records that could be combined with research data to reveal an individual's identity;

- the uniqueness of certain attributes of subjects; or

- inclusion of a variety of demographic characteristics on the subjects.

Information Not Protected

The following categories of information are not covered by the regulations and, as such, may be released in identifiable form for any purpose:

- o information obtained from records designated under State or Federal statute as "public" (exempted to preclude conflict with State open-record policies and "sunshine" legislation);
- o information regarding future criminal conduct (exempted to preclude conflict with Federal and/or State law);
- o information gathered for intelligence or law enforcement purposes (exempted to ensure that "intelligence" data are not included as "research and statistical information").

In addition, where identifiable data is obtained from *non-public* records for research/statistical purposes, the regulations apply to the extracted research/statistical data *only*. This exemption is specifically stated to preclude law enforcement concern over the possible extension of applicability of confidentiality regulations to administrative or criminal history record systems from which data is released.

It should be noted that the regulations do not require disclosure of the information described above. Accordingly, researchers may *voluntarily* withhold disclosure of such information--recognizing, however, that where such information is sought pursuant to a subpoena, information would not be protected by the immunity provision of the act and regulations.

Authorized Uses and Transfers of Data

The regulations provide that identifiable research/statistical data may only be used or revealed--on a need-to-know basis--as follows:

- for other research or statistical purposes;
- for any purposes authorized by the individual subject;
- to employees of the recipient of assistance;
- to subcontractors (provided subcontracts contain provisions to ensure security, confidentiality, and return of identifiable data); and
- to LEAA--for limited statutory reporting and auditing purposes.

The regulations do not:

- limit eligible recipients of data for research/statistical purposes or require that researchers be certified or licensed for the purpose of obtaining data;
- *require* that data--in identifiable or nonidentifiable form--be transferred for secondary use;
- require that LEAA approval be obtained prior to transfer of data.

Transfer for Research/Statistical Purposes

Information may be transferred or revealed in identifiable form for any research or statistical purpose. To ensure confidentiality of the information, however, the regulations require that:

- Information may only be transferred in identifiable form on a *need-to-know basis* (thus requiring that identifiers be stripped where transferred data can be utilized without identifiers).

- Information may only be *re*transferred where data are included in the recipient's data base and transfer is approved by the original transferor of data.

- Information must be returned upon conclusion of the project for which data is transferred unless alternative arrangements, consistent with the regulations, are agreed upon.

- Information may only be transferred pursuant to a *transfer agreement* binding the recipient of data to the restrictions of the regulations.

- Information may only be transferred upon a finding by the transferor that:

  - the proposed research use will not cause social or economic harm to the individuals identified in the data to be transferred;

  - the proposed project will be designed to ensure confidentiality; and

  - adequate administrative and physical security of data will be maintained by the recipient of the data.

Transfer with Consent of the Individual

The regulations provide that identifiable information may be revealed or transferred for nonresearch or statistical purposes where prior consent has been obtained from the individual to whom the information relates.

- Issues relating to consent (e.g., competence of consenting individual, persons authorized to consent for minors, etc.) will be determined pursuant to applicable State law.

- Subject consent may *generally* be obtained at any time prior to release or use for nonresearch/statistical purposes (including at the time of data collection).

- Where the data are sought for use in a judicial or administrative proceeding, however, written consent must be obtained at the time that the data are sought for use in such proceedings.

- Although not specifically stated in the regulations, it is recommended that all consent be obtained in written form and that copies of the consent be retained by both the persons releasing and receiving the data.

Subject Notification Requirements

The regulations distinguish among situations in which:

- o data are obtained *directly* from the subject through questionnaire or other direct inquiry;
- o data are developed through *observation* of subject activity; or
- o data are derived from *existing* records.

Specifically, the regulations require that:

Direct inquiry: Where data are obtained through direct subject inquiry, subjects must be advised, either orally or in writing, that information will, in the absence of alternative notification and consent, be used for research or statistical purposes only and that participation is (or is not) voluntary.

Subject observation: Where data are obtained through direct subject observation, subjects must be advised of the above-noted facts as well as the types of information to be collected.

Existing records: Where data are obtained from existing records, no notification of subjects is required. (Data obtained in this manner are, however, in all other respects covered by the provisions of the regulations.)

Waiver of Notification

Subject notification requirements may be waived where information is to be obtained through direct observation and, in the view of the researcher, notification would preclude or seriously impede conduct of the project. In such cases a justification for the waiver must be included as part of the privacy certificate.

"Unique" Subjects

Where data are obtained directly from a subject, the subject must be advised if it appears--by virtue of sample size or subject uniqueness--that identity cannot be reasonably concealed. In such cases, agreement to participate in the study is deemed to constitute consent to revelation of data in potentially identifiable form in research/statistical products of the project. Agreement to participate does not, however, without additional specific consent, authorize disclosure of the data for nonresearch/statistical uses.

Security of Data

The regulations require that physical and administrative security of identifiable research/statistical data be ensured by the original researcher and by all subsequent recipients of data.

To accomplish this objective, the researcher must:

- notify all staff (paid or volunteer) of the requirements of the regulations and obtain written agreement therewith from all employees;

- limit staff access to identifiable data on a "need-to-know" basis;

- maintain data under physical conditions designed to preclude intentional or accidental access to data by nonauthorized individuals.

- maintain a log indicating all transfers of information in identifiable form. (The log should indicate the name of the individual to whom the information was released, the individual's organization, the date of dissemination, identification of records released, and the purpose for which the transfer was made.)

To ensure proper administrative security, it is also recommended that a list of all individuals (including employees) *authorized* to have direct access to the identifiable data base be developed and that a record of *actual access* to identifiable information by these authorized users be maintained.

Computer Storage

Where identifiable data are to be maintained in a computer, the researcher must obtain written assurances that adequate hardware and software and administrative procedures will be utilized to:

- ensure technical security of data;
- preclude unauthorized access to identifiable data; and
- prevent unauthorized linkage of data.

There is no requirement that data be stored in a "dedicated" system or that data be entered in the computer in nonidentifiable form.

Immunity

The regulations (in Sec 22.28) follow the language of the act and provide that:

> "Copies of research or statistical information identifiable to a private person shall be immune from legal process and shall only be admitted as evidence or used for any purpose in any action, suit, or other judicial or administrative proceeding with the written consent of the individual to whom the data pertains."

In interpreting the immunity provisions, the following should be noted:

- The statute provides for an automatic immunity, requiring no action by the researcher or LEAA.

- Immunity applies to "copies" of data--and accordingly, would not apply to researcher recollections of information, nonrecorded impressions of subject response, etc.

- Immunity applies regardless of whether or not subjects are notified of project participation or of the immunity protections.

- Immunity is only applicable to "administrative" and "judicial" proceedings and accordingly would not protect against release of data in legislative proceedings.

- Immunity is based on the Federal statute and not merely on the language of the regulations or a grant condition.

- Immunity applies to research/statistical information collected after August 1973 (LEAA-funded) and October 3, 1977 (JJDP-funded)--regardless of whether or not the project received additional funding after that date.

- Immunity applies to Federal and State court or administrative proceedings.

Final Disposition of Data

Upon termination of a project in which identifiable data were collected, the regulations provide two options with respect to final disposition of data.

Specifically:

- o Data, or all identifying portions thereof, may be destroyed.

- o Identifiers may be stripped from data and a name-index retained under separate and secure conditions.

Removal of identifiers and maintenance of a separate name-index code will permit subsequent longitudinal studies and/or reanalysis of data. Where the name-index procedure is to be followed, a description of the separate maintenance conditions for the name-index must be included in the privacy certificate.

In planning for the final disposition of data, researchers should be aware that Federal or State requirements may preclude the destruction of records for a specific period of years from the completion of the project. In such cases the name-stripping process should be utilized during this period.

Disposition of Transferred Data

Identifiable data transferred to a subsequent researcher pursuant to a transfer agreement must be returned to the original researcher at project conclusion unless alternative arrangements are agreed upon. Such arrangements must include, *as a minimum,* the maintenance of a separate and secure name-index code.

Procedural Requirements

PRIVACY CERTIFICATE
TRANSFER AGREEMENT

The procedural mechanisms through which the regulations will be implemented are the *privacy certificate* and the *transfer agreement.*

Copies of a sample privacy certificate and sample transfer agreement are included at the end of this document. These forms are *samples only.* Alternative forms may also be used so long as they contain the necessary assurances.

The Privacy Certificate

The regulations require that a privacy certificate be submitted as part of any application for a project in which data identifiable to a private person will be collected for research or statistical purposes. A certificate must, therefore, be submitted in connection with research/statistical projects and with those "action" projects which include an evaluation component involving the collection of data identifiable to a private person. A certificate would not be required in projects in which data is to be collected in nonidentifiable, statistical form only.

Contents of Privacy Certificate

The privacy certificate should contain assurances that:

- Limitations on use/revelation/transfer of identifiable data will be maintained.
- Adequate administrative and physical security procedures will be undertaken.
- The project and any project reports will be designed to ensure confidentiality of data.
- Appropriate subject notification procedures will be followed.
- Dissemination log procedures will be followed to control release of identifiable data.

To support these assurances, the privacy certificate should briefly describe:

- o procedures to ensure confidentiality of data;
- o procedures to ensure physical/administrative security of data;
- o procedures for subject notification and/or justification for waiver thereof (pursuant to Sec 22.27(c) of the regulations); and
- o procedures for final disposition of data (including security arrangements where separate name-index codes will be maintained).

The certificate should also include the name and title of:

- o the individual to be charged with primary responsibility for ensuring compliance with the regulations (generally, the project director);
- o the individual authorized to approve transfers of data (and any institutional limitations associated with data transfer); and
- o the individual authorized to determine final disposition procedures for data developed in the project.

Where relevant, a copy of consent forms should also be attached to the certificate.

Submission of Privacy Certificate

A privacy certificate should be submitted as part of any application for a project to be funded under the Omnibus Crime Control and Safe Streets Act in which research/statistical data identifiable to a private person is to be collected.

Where applicants do not initially anticipate that research/statistical data will be collected in identifiable form, a privacy certificate should be submitted and approved at such time as funds are, in fact, to be expended for collection of identifiable research/statistical data. In such cases, a special condition may be included in the grant providing as follows:

> "Where a privacy certificate is not initially submitted, such a certificate must be submitted and approved prior to the expenditure of LEAA funds for collection of identifiable research/statistical data."

Privacy certificates may be amended at any time, subject to approval by the appropriate reviewing official or board.

The Transfer Agreement

The transfer agreement is intended to ensure the confidentiality of identifiable information which is transferred from the original LEAA supported researcher to a subsequent researcher. Although a transfer agreement is required in connection with each transfer of data, successive transfers of data to the same recipient may be handled through amendments to an original agreement.

Contents of Transfer Agreement

The information and assurances to be included in the transfer agreement are indicated in the sample transfer agreement which is included at the end of this document. Where institutional regulations require that additional assurances be obtained in connection with transfer of data, such assurances must also be addressed prior to transfer of data.

The transfer agreement should be signed by the individual authorized to transfer identifiable data protected under the regulations, as indicated in the original privacy certificate.

As in the case of the privacy certificate, the transfer agreement should designate the individual or official of the recipient organization who will have primary responsibility for maintenance of transferred data.

Submission and Review of Transfer Agreement

A transfer agreement must be entered into prior to transfer of data in identifiable form for subsequent research/statistical uses.

A transfer agreement is not required where data is transferred to a sub-contractor, provided that provisions assuring security and nonrevelation of data, (consistent with requirements of the regulations), are included in the sub-contract agreement.

It is recommended that a copy of the transfer agreements be retained by both the transferor and the recipient of data. Copies of the transfer agreement are not required to be submitted to or approved by LEAA.

Where information is to be retransferred by a recipient of data, the transfer agreement between primary and secondary recipient of data should be reviewed by the original researcher prior to approval of the secondary transfer.

Interface with LEAA Regulations on Criminal History Information Systems (28 CFR Part 20)

The LEAA regulations covering Privacy and Security of Criminal History Information (28 CFR Part 20) provide that agencies covered by the regulations may, but are not required, to disclose identifiable criminal history information for a research or statistical purpose. Such disclosure is permitted regardless of whether or not the proposed research or statistical activity is LEAA supported.

Where criminal history information is released for such purposes, an agreement ensuring confidentiality of the data must be entered into between the criminal justice agency and the recipient of the data. Where data recipients have submitted a privacy certificate in connection with the project for which the criminal history information is to be used, the certificate would be sufficient to fulfill this requirement. If no privacy certificate has been submitted (e.g., if the research is not LEAA-supported), the agreement should contain assurances similar to those required for the privacy certificate.

Agencies subject to 28 CFR Part 20 should note that release of data for a research/statistical purpose does not subject the agency to provisions of the confidentiality regulations (28 CFR Part 22). This is the case since the confidentiality provisions apply only to data which are obtained for research/statistical purposes and not to be basic records from which such data is extracted.

SUGGESTED FORMAT--SAMPLE ONLY

PRIVACY CERTIFICATION

Title of Project

Name of Grantee

The Privacy Certification should contain the following information:

I. A description of the Research/Statistical component of project (or if this information is contained in the grant proposal, a notation of where in the grant proposal the information is located). If questionnaires are to be utilized, attach copy.

II. A justification for collection and/or maintenance of data in identifiable form and description of procedures to be followed to preserve anonymity of private persons as required by Sec. 22.23(b)(7).

III. A description of physical and/or administrative procedures to be followed to insure the confidentiality of data (including procedures for notification of staff and sample staff notification agreement as required by Sec. 22.23(b)(2)).

IV. A description of the procedures to be used for notification of subjects as required by Sec. 22.23(b)(4), or if such notification is to be waived, pursuant to Sec. 22.27(c) a justification therefore.

Where identifiable information is to be used for non-research or statistical purposes, a sample or description of the Consent Statement to be used, shall be attached.

V. A sample of the Transfer Agreement to be used for transfer of data in identifiable form. Indicate the name and title of the individual with the authority to transfer data. Also describe any institutional limitations or restrictions applicable to such transfers.

VI. A description of procedures to be followed for final disposition of data, and where a name index is to be maintained, a description of procedures to secure the index as required by Sec. 22.25(b). Indicate the name and title of the individual authorized to determine the final disposition of data.

The Certification should also contain an assurance such as the following:

Grantee certifies that:

(1) the information contained above is correct and that the procedures noted above will be carried out;

(2) the project will be conducted, consistent with all requirements of Sec. 524(a) of the Omnibus Crime Control Act of 1968, as amended, and Regulations promulgated thereunder contained in 28 CFR Part 22;

(3) LEAA will be notified of any material changes in any of the information supplied above.

Signature of person authorized to sign for grantee

Signature and title of project director or other official primarily responsible for use and maintenance of confidential data (if same as above, indicate)

Date

SUGGESTED FORMAT--SAMPLE ONLY

Information Transfer Agreement

Title of Project for which information was originally compiled, obtained, or used

Name of Individual or Organization to which information is being transferred

LEAA Grant or Contract Number

- Title of Project for which data will be used

The transfer agreement should contain the following information:

I. A description of the Research/Statistical component of the project and a statement of how the project plan will be designed to preserve the anonymity of private persons to whom the information relates.

II. An assurance that the recipient of data is familiar with the Department of Justice regulations, (28 CFR Part 22), and agrees to comply with them.

III. An assurance that information identifiable to a private person that is transferred pursuant to this agreement will be used for research and statistical purposes only and will not be revealed except as allowed under §22.24(b), (e) of the regulations--project findings and reports prepared for dissemination will also not contain such information.

IV. A description of the administrative and physical precautions that will be taken to assure security of information obtained.

V. An assurance that the final disposition of the information transferred has been determined by the parties to this agreement and is in accord with §22.24(h). This should include a description of the procedures.

The recipient agrees that any violation of this agreement will constitute a violation of the Department of Justice regulations, and be punishable as such.

Signature of person authorized to transfer this data

Signature of person receiving data and assuming responsibility for its confidentiality and security

☆ U. S. GOVERNMENT PRINTING OFFICE: 1978—260-997/6

END