Secretary to carry out quality assessments, medical audits or utilization review.

3. Disclosure may be made to a congressional office from the record of an individual in response to an inquiry from the congressional office made at the request of that individual.

4. The Department may disclose information from this system or records to the Department of Justice, to court or other tribunal, or to another party before such tribunal, when (a) HHS, or any component thereof; or (b) any HHS employee in his or her official capacity; or (c) any HHS employee in his or her individual capacity where the Department of Justice (or HHS, where it is authorized to do so) has agreed to represent the employee; or (d) the United States or any agency thereof where HHS or any of its components, is a party to litigation or has an interest in such litigation, and HHS determines that the use of such records by the Department of Justice, the tribunal, or the other party is relevant and necessary to the litigation and would help in the effective representation of the governmental party, provided, however, that in each case, HHS determines that such disclosure is compatible with the purpose for which the records were collected.

# POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:

### STORAGE:

Data may be stored in file folders, bound notebooks, or computeraccessible media (e.g., magnetic tapes or discs).

# RETRIEVABILITY:

Information is retrieved by name and/ or participant identification number within each evaluation study. There is no central collection of records in this system, and no central means of identifying individuals whose records are included in the separate sets of records that are maintained for particular evaluation studies.

#### SAFEGUARDS:

A variety of safeguards are implemented for the various sets of records in this system according to the sensitivity of the data each set contains. information already in the public domain, such as titles and dates of publications, is not restricted. However, sensitive information, such as personal or medical history or individually identified opinions, is protected according to its level of sensitivity. Records derived from other systems of records will be safeguarded at a level at least as stringent as that required in the original systems. Minimal safeguards for the protection of information which is not available to the general public include the following:

1. Authorized users: Regular access to information in a given set of records is limited to NIH or to contractor employees who are conducting, reviewing or contributing to a specific evaluation study. Other access is granted only on a case-by-case basis, consistent with the restrictions required by the Privacy Act (e.g., when disclosure is required by the Freedom of Information Act), as authorized by the system manager or designated responsible official.

2. Physical safeguards: Records are stored in closed or locked containers, in areas which are not accessible to unauthorized users, and in facilities which are locked when not in use. Records collected in each evaluation project are maintained separately from those of other projects. Sensitive records are not left exposed to unauthorized persons at any time. Sensitive data in machine-readable form may be encrypted.

3. Procedural safeguards: Access to records is controlled by responsible employees and is granted only to authorized individuals whose identities are properly verified. Data stored in mainframe computers is accessed only through the use of keywords known only to authorized personnel. When personal computers are used, magnetic media (e.g. diskettes) are protected as under Physical Safeguards. When data is stored within a personal computer (i.e., on a "hard disk"), the machine itself is treated as though it were a record, or records, under Physical Safeguards. Contracts for operation of this system of records require protection of the records in accordance with these safeguards; NIH project and contracting officers monitor contractor compliance.

These practices are in compliance with the standards of Chapter 45–13 of the HHS General Administration Manual, "Safeguarding Records Contained in Systems of Records," supplementary Chapter PHS hf: 45–13, and Part 6, "ADP Systems Security," of the HHS Information Resources Management Manual and the National Institute of Standards and Technology Federal Information Processing Standards (FIPS Pub. 41 and FIPS Pub. 31).

### RETENTION AND DISPOSAL:

Records are retained and disposed of under the authority of the NIH Records Control Schedule contained in NIH Manual Chapter 1743, Appendix 1"Keeping and Destroying Records" (HHS Records Management Manual, Appendix B–361), item 1100–C–2. Refer to the NIH Manual Chapter for specific disposition instructions.

### SYSTEM MANAGER(S) AND ADDRESS:

See Appendix 1.

Policy coordination for this system is provided by:

Associate Director, Office of Strategic Planning and Evaluation, Office of Science Policy and Technology Transfer, National Institutes of Health, 6006 Executive Boulevard, Suite 312, Rockville, MD 20892.

# NOTIFICATION PROCEDURE:

To determine if a record exists, write to the official of the organization responsible for the evaluation, as listed in Appendix 2. If you are not certain which component of NIH was responsible for the evalaution study, or if you believe there are records about you in several components of NIH, write to:

NIH Privacy Act Officer, Building 31, Room 1B25, 9000 Rockville Pike, Bethesda, MD 20892.

Requesters must provide the following information:

1. Full name, and name(s) used while studying or employed;

2. Name and location of the evaluation study or other NIH program in which the requester participated or the institution at which the requester was a student or employee, if applicable;

3. Approximate dates of participation, matriculation or employment, if applicable.

The requester must also verify his or her identity by providing either a notarization of the request or a written certification that the requester is who he or she claims to be and understands that the knowing and willful request for acquisition of a record pertaining to an individual under false pretenses is a criminal offense under the Act, subject to a five thousand dollar fine.

An individual who requests notification of or access to a medical record shall, at the time the request is made, designate in writing, a responsible representative, who may be a physician, other health professional, or other responsible individual, who will be willing to review the record and inform the subject individual of its contents at the representative's discretion.

A parent or guardian who requests notification of, or access to, a child's or incompetent person's medical record shall designate a family physician or