SYSTEM LOCATION:

Westwood Building, 5333 Westbard Avenue, Bethesda, MD 20892, and Building 12, NIH Computer Center, 9000 Rockville Pike, Bethesda, MD 20892.

For information pertaining to the chartered advisory committees of the National Institutes of Health: Building 31, Room 3B–55, 9000 Rockville Pike, Bethesda, MD 20892.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Applicant and Principal Investigators; Program Directors; NRSA Trainees and Fellows; Research Career Awardees; and Chartered Advisory Committee members.

CATEGORIES OF RECORDS IN THE SYSTEM:

Applications, awards, associated records, trainee appointments, and current and historical information pertaining to chartered advisory committees.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

42 U.S.C. 241c, 58 Stat. 691c & d repealed.

PURPOSE(S):

(1) To support centralized grant programs of the Public Health Service. Services are provided in the areas of grant application assignment and referral, initial review, council review, award processing and grant accounting. The data base is used to provide complete, accurate, and up-to-date reports to all levels of management.

(2) To maintain communication with former fellows and trainees who have incurred a payback obligation through the National Research Service Award Program.

(3) To maintain current and historical information pertaining to the establishment of chartered advisory committees of the National Institutes of Health and the appointment or designation of their members.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

1. Disclosure may be made to the National Technical Information Service (NTIS), Department of Commerce, for dissemination of scientific and fiscal information on funded awards (abstract of research projects and relevant administrative and financial data).

2. Disclosure may be made to the cognizant audit agency for auditing.

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. Disclosure may be made to qualified experts not within the definition of Department employees as prescribed in Department Regulations for opinions as a part of the application review process.

5. Disclosure may be made to a Federal agency, in response to its request, in connection with the letting of a contract, or the issuance of a license, grant or other benefit by the requesting agency, to the extent that the record is relevant and necessary to the requesting agency's decision in the matter.

6. A record may be disclosed for a research purpose, when the Department: (A) Has determined that the use or disclosure does not violate legal or policy limitations under which the record was provided, collected, or obtained; (B) has determined that the research purpose (1) cannot be reasonably accomplished unless the record is provided in individually identifiable form, and (2) warrants the risk to the privacy of the individual that additional exposure of the record might bring; (C) has required the recipient to (1) establish reasonable administrative, technical, and physical safeguards to prevent unauthorized use or disclosure of the record, (2) remove or destroy the information that identifies the individual at the earliest time at which removal or destruction can be accomplished consistent with the purpose of the research project, unless the recipient has presented adequate justification of a research or health nature for retaining such information, and (3) make no further use or disclosure of the record except (a) in emergency circumstances affecting the health or safety of any individual, (b) for use in another research project, under these same conditions, and with written authorization of the Department, (c) for disclosure to a properly identified person for the purpose of an audit related to the research project, if information that would enable research subjects to be identified is removed or destroyed at the earliest opportunity consistent with the purpose of the audit, or (d) when required by law; (D) has secured a written statement attesting to the recipient's understanding of, and willingness to abide by these provisions.

7. The Department contemplates that it may contract with a private firm for the purpose of collating, analyzing, aggregating or otherwise refining records in this system. Relevant records will be disclosed to such a contractor. The contractor will be required to maintain Privacy Act safeguards with respect to such records. 8. Disclosure may be made to the grantee institution in connection with performance or administration under the conditions of the award.

9. Disclosure may be made to the Department of Justice, or to a court or other tribunal, from this system of records 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 determines that the litigation is likely to affect HHS or any of its components, is a party to litigation or has any interest in such litigation, and HHS determines that the use of such records by the Department of Justice, court or other tribunal 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:

Records are stored on discs and magnetic tapes.

RETRIEVABILITY:

Records are retrieved by name, application, grant or contract ID number.

SAFEGUARDS:

1. Authorized users: Employees who maintain records in this system are instructed to grant regular access only to PHS extramural and committee management staff. Other one-time and special access by other employees is granted on a need-to-know basis as specifically authorized by the system manager.

2. *Physical safeguards:* Physical access to DRG work areas is restricted to DRG employees.

3. *Procedural safeguards:* Access to source data is strictly controlled by files staff. Records may be removed from files only at the request of the system manager or other authorized employee. Access to computer files is controlled by the use of registered accounts, registered initials, keywords, etc. The computer system maintains an audit record of all attempted and successful requests for access.

These practices are in compliance with the standards of Chapter 45–13 of