(AHCPR), and the Health Care Financing Administration (HCFA).

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

1. 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; e.g., disclosure of alcohol or drug abuse patient records will be made only in accordance with the restrictions of confidentiality statutes and regulations (42 U.S.C. 290 (dd-2), 42 U.S.C. 241 and 405, 42 CFR part 2), and where applicable, no disclosures will be made inconsistent with an authorization of confidentiality under 42 U.S.C. 242a and 42 CFR part 2a; (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; and (D) has secured a written statement attesting to the recipient's understanding of, and willingness to abide by, these provisions. Examples of organizations and agencies of which records from this system may be disclosed include, but are not limited to Health Maintenance Organizations (HMOs) and other service providers participating in the studies and various federal and state agencies, such as the Veteran's Administration, branches of the Armed Forces, and state and local health department.

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

3. In the event of litigation, where the defendant is (a) the Department, any component of the Department, or any employee of the Department in his or her official capacity; (b) the United States where the Department determines that the claim, if successful, is likely to directly affect the operations of the Department or any of its components; or (c) any Department employee in his or her individual capacity where the Justice Department has agreed to represent such employee, for example, in defending a claim against the Public Health Service, based upon an individual's mental or physical condition and alleged to have arisen because of activities of the Public Health Service in connection with such an individual, the Department may disclose such records as it deems desirable or necessary to the Department of Justice to enable that Department to present an effective defense, provided such disclosure is compatible with the purpose for which the records were collected.

4. ODPHP may contract with a private firm for the purpose of collecting, analyzing, aggregating, or otherwise refining records in this system. Relevant records may be disclosed to such contractor. The contractor shall be required to maintain Privacy Act safeguards with respect to such records.

5. Disclosure may be made to organizations deemed qualified by the Secretary to carry out quality assessments, medical audits or utilization review.

6. Information from this system may be disclosed to Federal agencies, State agencies (including the Motor Vehicle Administration and State vital statistics offices), private organizations, and other third parties (such as current or prior employers, acquaintances, relatives), in order to obtain information on morbidity and mortality experiences and to locate individuals for follow-up studies. Social Security numbers may be disclosed to the Social Security Administration to ascertain disabilities and/or location of participants. Social Security numbers may also be given to other Federal agencies, and State and local agencies for purposes of locating individuals for participation in followup studies.

7. Records may be disclosed to student volunteers, individuals working under a personal services contract, and other individuals performing functions for PHS who do not technically have the status of agency employees, if they need the records in the performance of their agency functions.

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

STORAGE:

Records may be stored in hard copy, index cards, file folders, computer tapes and disks (including optical disks), photography media, microfiche, microfilm, and audio and video tapes. Typically, factual data with study code numbers are stored on computer tape or disk, while the key to personal identifiers is stored separately, without factual data, in locked paper files.

RETRIEVABILITY:

During data collection stages and follow-up retrieval is by personal identifier (e.g., name, Social Security Number, medical record or study identification number etc.). During the data analysis stage, data are normally retrieved by the variables of interest (e.g., diagnosis, age, occupation).

SAFEGUARDS:

1. Authorized Users: Access to identifiers and to link files is strictly limited to the authorized personnel whose duties require such access. Procedures for determining authorized access to identified data are established as appropriate for each location. Personnel, including contractor personnel, who may be so authorized include those directly involved in data collection and in the design of research studies, e.g., interviewers and interviewer supervisors; project managers, and statisticians involved in designing sampling plans.

Other one-time and special access by other employees is granted on a need-to-know basis as specifically authorized

by the System Manager.

Researchers authorized to conduct research will typically access the system through the use of encrypted identifiers sufficient to link individuals with records in such a manner that does not compromise confidentiality of the individual.

2. Physical Safeguards: Records are stored in locked rooms, locked file cabinets, and/or secured computer facilities. Personal identifiers and link files are separated as much as possible and stored in locked files. Computer data access is limited through the use of key words known only to authorized personnel.

A separate key list linking ID codes to respondents will be maintained by the contractor conducting the survey,