ATTACHMENT F: Epidemic Investigation Case Records System Notice

Epidemic Investigation Case Records System Notice

System name: Epidemic Investigation Case Records. HHS/CDC/NCID.
Security classification: None.
System location: National Center for Infectious Diseases, Bldg. 1, Rm. 6013, Centers for Disease Control and Prevention, 1600 Clifton Road, NE, Atlanta, GA 30333; 4055 Tudor Centre Drive, Anchorage, Alaska 99508; Division of Vector-Borne Infectious Diseases, Post Office Box 2087 (Foot Hills Campus), Fort Collins, CO 80522; Dengue Branch (San Juan Laboratories), National Center For Infectious Diseases, Centers For Disease Control and Prevention, Calle Casia 2, San Juan, Puerto Rico 00921.

Epidemic Intelligence Service, Centers for Disease Control and Prevention, 1600 Clifton Road, MS E92, Atlanta, GA 30333.

National Center for HIV, STD and TB Prevention, Corporate Square, Bldg. 11, Rm. 2106, Centers for Disease Control and Prevention, 1600 Clifton Road, NE, Atlanta, GA 30333.

National Center for Environmental Health, Chamblee Bldg. 101, Rm. 3116, Centers for Disease Control and Prevention, 4770 Buford Highway, NE, Atlanta, GA 30341-3724.

National Center for Injury Prevention and Control, Koger/Vanderbilt Building, Rm. 1017B, Centers for Disease Control and Prevention, 4770 Buford Highway, NE, Atlanta, GA 30341-3724.

National Immunization Program, Corporate Square, Bldg. 12, Rm. 5113, Centers for Disease Control and Prevention, 1600 Clifton Road, NE, Atlanta, GA 30333.
and

Federal Records Center, 1557 St. Joseph Avenue, East Point, GA 30344.

Categories of individuals covered by the system: Adults and children with disease and other health conditions of public health significance, their contacts, others with possible exposure and appropriate controls.

Categories of records in the system: Medical histories, case reports.

Authority for maintenance of the system: Public Health Service Act, Section 301, "Research and Investigation," (42 U.S.C. 241); Sections 304, 306, and 308(d), which discuss authority to grant assurances of confidentiality for health research and related activities (42 U.S.C. 242 b, k, and m(d)); and Section 361, "Quarantine and Inspection, Control of Communicable Diseases," (42 U.S.C. 264).

Purpose(s): The record system is used by professional staff at the Centers for Disease Control and Prevention (CDC) for more complete knowledge of the disease/condition in the following ways: (1) An examination of existing files enables investigators to determine areas that have been adequately investigated and to specify those that might be pursued; or (2) Records may later be examined in the light of future discoveries and proven associates so that relevant data collected at the time of the outbreak may be analyzed and reassessed. CDC may or may not request duplicate copies of these State and/or local health department records for further analysis following completion of the field investigation.

Routine uses of records maintained in the system, including categories of users and the purposes of such uses: The following routine uses apply to all records in this system except those maintained under an assurance of confidentiality provided by Section 308(d) of the Public Health Service Act (unless

expressly authorized in the consent form or stipulated in the Assurance Statement):
These records may be disclosed, i.e., returned to the State and/or local health departments in order for them to take measures to control, prevent, or treat disease and to conduct follow-up activities with patients and others contacted during the investigations. Private physicians may also be supplied pertinent medical information on their patients from these records.
Disclosure may be made to a congressional office from the record of an individual in response to a verified inquiry from the congressional office made at the written request of that individual.
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 Department of Justice 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 individual, disclosure may be made to the Department of Justice to enable that Department to present an effective defense, provided 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: File folders, cards, and computer tapes/disks and printouts.

Retrievability: Retrieved alphabetically by name.

Safeguards:

1. Authorized Users: A database security package is implemented on CDC's mainframe computer to control unauthorized access to the system. Attempts to gain access by unauthorized individuals are automatically recorded and reviewed on a regular basis. Access is granted to only a limited number of physicians, scientists, statisticians, and designated support staff of the Centers for Disease Control and Prevention (CDC), or its contractors, as authorized by the system manager to accomplish the stated purposes for which the data in this system have been collected.

2. Physical Safeguards: Access to the CDC Clifton Road facility where the mainframe computer is located is controlled by a cardkey system. Access to the computer room is controlled by a cardkey and security code (numeric keypad) system. Access to the data entry area is also controlled by a cardkey system. The hard copy records are kept in locked cabinets in locked rooms. The local fire department is located next door to the Clifton Road buildings. The computer room is protected by an automatic sprinkler system, automatic sensors (e.g., water, heat, smoke, etc.) are installed, and portable fire extinguishers are located throughout the computer room. The system is backed up on a nightly basis with copies of the files stored off site in a secure fireproof safe. The 24-hour guard service in buildings provides personnel screening of visitors. Electronic anti-intrusion devices are in effect at the Federal Records Center.

3. Procedural Safeguards: Protection for computerized records both on the mainframe and the CIO Local Area Network (LAN) includes programmed verification of valid user identification code and password prior to logging on to the system, mandatory password changes, limited log-ins, virus protection, and user rights/file attribute restrictions. Password protection imposes user name and password log-in requirements to prevent unauthorized access. Each user name is assigned limited access rights to files and directories at varying levels to control file sharing. There are routine daily backup procedures and

Vault Management System for secure off-site storage is available for backup tapes. To avoid inadvertent data disclosure, “degaussing” is performed to ensure that all data are removed from Privacy Act computer tapes and/or other magnetic media. Additional safeguards may be built into the program by the system analyst as warranted by the sensitivity of the data. CDC and contractor employees who maintain records are instructed to check with the system manager prior to making disclosures of data. When individually identified data are being used in a room, admittance at either CDC or contractor sites is restricted to specifically authorized personnel. Privacy Act provisions are included in contracts, and the CDC Project Director, contract officers and project officers oversee compliance with these requirements. Upon completion of the contract, all data will be either returned to CDC or destroyed, as specified by the contract.

4. Implementation Guidelines: The safeguards outlined above are developed in accordance with Chapter 45-13, "Safeguarding Records Contained in Systems of Records," of the HHS General Administration Manual; and Part 6, "Automated Information System Security," of the HHS Information Resources Management Manual. FRC safeguards are in compliance with GSA Federal Property Management Regulations, Subchapter B--Archives and Records. Data maintained in CDC Atlanta’s Processing Center are in compliance with OMB Circular A-130, Appendix III. Security is provided for information collection, processing, transmission, storage, and dissemination in general support systems and major applications. The CIO LANs currently operate under Novell Netware v 4.11 and are in compliance with “CDC & ATSDR Security Standards for Novell File Servers.”

5. Retention and disposal: Records are maintained in agency for four years. Disposal methods include erasing computer tapes, burning or shredding paper materials or transferring records to the Federal Records Center when no longer needed for

evaluation and analysis. Records destroyed by paper recycling process when 20 years old, unless needed for further study.
6. System manager(s) and address: Director, National Center for Infectious Diseases, Bldg. 1, Rm. 6013, MS C12, Centers for Disease Control and Prevention, 1600 Clifton Road, NE, Atlanta, GA 30333.

Director, Epidemic Intelligence Service, MS E92, Centers for Disease Control and Prevention, 1600 Clifton Road, NE, Atlanta, GA 30333.

Director, National Center for HIV, STD and TB Prevention, Corporate Square, Bldg. 11, Rm. 2106, MS E07, Centers for Disease Control and Prevention, 1600 Clifton Road, NE, Atlanta, GA 30333.

Director, National Center for Environmental Health, Chamblee Bldg. 101, Rm. 3116, MS F29, Centers for Disease Control and Prevention, 4770 Buford Highway, NE, Atlanta, GA 30341-3724.

Director, National Center for Injury Prevention and Control, Koger/Vanderbilt Building, Rm. 1017B, MS K02, Centers for Disease Control and Prevention, 4770 Buford Highway, NE, Atlanta, GA 30341-3724.

Director, National Immunization Program, Corporate Square, Bldg. 12, Rm. 5113, MS E05, Centers for Disease Control and Prevention, 1600 Clifton Road, NE, Atlanta, GA 30333.

Policy coordination is provided by: Associate Director for Management and Operations, Bldg. 16, Rm. 5117, MS D15, Centers for Disease Control and Prevention, 1600 Clifton Road, NE, Atlanta, GA 30333.

Notification procedure: An individual may learn if a record exists about himself or herself by contacting the system manager at the address above. Requesters in person must provide driver's

license or other positive identification. Individuals who do not appear in person must either: (1) submit a notarized request to verify their identity; or (2) certify that they are the individuals they claim to be and that they understand that the knowing and willful request for or acquisition of a record pertaining to an individual under false pretenses is a criminal offense under the Privacy Act subject to a $5,000 fine.

An individual who requests notification of or access to medical records shall, at the time the request is made, designate in writing a responsible representative who is 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 medical record shall designate a family physician or other health professional (other than a family member) to whom the record, if any, will be sent. The parent or guardian must verify relationship to the child by means of a birth certificate or court order, as well as verify that he or she is who he or she claims to be.

The following information must be provided when requesting notification: (1) full name; (2) the approximate date and place of the study, if known; and (3) nature of the questionnaire or study in which the requester participated.

Record access procedures: Same as notification procedures. Requesters should also reasonably specify the record contents being sought. An accounting of disclosures that have been made of the record, if any, may be requested.

Contesting record procedures: Contact the official at the address specified under System Manager above, reasonably identify the record and specify the information being contested, the corrective action sought, and the reasons for requesting the correction, along with supporting information to show how the record is inaccurate, incomplete, untimely, or irrelevant.

Record source categories: Individuals, State and local health departments, and private physicians.

Systems exempted from certain provisions of the act: None.