SORN 09-20-0171

System Name: Quarantine- and Traveler-Related Activities, Including Records for Contact Tracing Investigation and Notification under 42 CFR Parts 70 and 71, HHS/CDC/CCID.

Security Classification: None.

System Location(s):

Division of Global Migration and Quarantine, National Center for the Preparedness, Detection, and Control of Infectious Disease (NCPDCID), Coordinating Center for Infectious Diseases (CCID), Centers for Disease Control and Prevention, 1600 Clifton Road, NE., Building 16; MS E03, Atlanta, GA 30333.

Records may occasionally be stored at Quarantine Stations located at key ports of entry and at contractor sites.

Categories of Individuals Covered by the System: Individuals subject to quarantine or isolation orders, ill travelers (i.e., passengers and crew), contacts of ill travelers, and/or individuals exposed or suspected of being exposed to serious communicable

diseases.

Categories of Records in the System: Passenger and crew manifests from conveyances carrying individuals subject to 42 CFR parts 70 and 71, case reports, illness response forms, medical assessments, medical records (including but not limited to clinical, hospital and laboratory data and data from other relevant tests), name, address, date of birth, and related information and documents collected for the purpose of carrying out agency responsibilities under sections 311 and 361-368 of the Public Health Services Act.

Authority for Maintenance of the System: Sections 311, 361-368 of the Public Health Service Act.

Purpose(s): This system maintains records on the conduct of activities (e.g., quarantine, isolation) that fulfill HHS's and CDC's statutory authority under sections 311, 361-368 of the Public Health Service Act to prevent the introduction, transmission and spread of communicable diseases.

Records are collected when individual known or suspected to have been exposed to serious communicable diseases arrives into the United States from foreign countries or is engaged in interstate or international movement These records are used to (1) document reports of illness that may pose a public health risk occurring while on board airplanes, maritime vessels, and at land-border crossings of persons arriving from foreign countries or traveling between states; (2) perform contact tracing investigations and notifications of passengers and crew when known or suspected exposures to serious communicable diseases occur on board a conveyance arriving in the United States from a foreign country or traveling from one state or possession to another; (3) inform international, federal, state or local public health authorities so that these authorities may act to protect public health or safety; and (4) take such actions (e.g., quarantine or isolation) as necessary to prevent the introduction, transmission, and spread of serious communicable diseases from persons arriving into the United States from foreign countries or persons engaged in interstate or international movement.

Routine Uses of Records Maintained in the System, Including Categories of Users and the Purposes of such Uses:

(1) Records may be disclosed to contractors to handle program work duties, performing many of the same functions as FTEs within DGMQ in situations where additional staff is required. Contractors are required to maintain Privacy Act safeguards with respect to such records.

(2) Records may be disclosed to state and local health departments and other cooperating medical and public health authorities and their counsel to more effectively deal with outbreaks and other significant public health conditions.

(3) Personal information from this system may be disclosed as a routine use to appropriate conveyance personnel, Federal agencies, state and local health departments, Department of State and embassy personnel (U.S. and foreign), and health authorities in foreign countries for contact tracing investigations and notifications of possible exposures to serious communicable diseases in connection with travel.

(4) Records may be disclosed to the Department of Homeland Security to restrict travel of persons who pose a public health risk and in the instance of suspected domestic or international terrorism.

(5) Disclosure may be made to medical personnel providing evaluation and care for ill or exposed persons, including travelers.

(6) Records may be disclosed to the World Health Organization in accordance with U.S. responsibilities as a signatory to the International Health Regulations or other international agreements.

(7) Personal information may be disclosed to federal, state, and local authorities for taking necessary actions to place someone under quarantine or isolation, for enforcement of other quarantine regulations, or to protect the public's health and safety.

(8) Records may be disclosed to cooperating state and local legal departments enforcing concurrent legal authority related to quarantine or isolation activities.

(9) In the event that a system of records maintained by this agency to carry out its functions indicates a violation or potential violation of law, whether civil, criminal or regulatory in nature, and whether arising by general statute or particular program

statute, or by regulation, rule or order issued pursuant thereto, the relevant records in the system of records may be referred, as a routine use, to the appropriate agency, whether federal, foreign, state or local, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute, or rule, regulation or order issued pursuant thereto.

(10) 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

(11) 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, disclosure may be made to the Department of Justice to enable that Department to present an effective defense.

(12) Records may be disclosed to appropriate Federal agencies and Department contractors that have a need to know the information for the purpose of assisting the Department's efforts to respond to a suspected or confirmed breach of the security or confidentiality of information disclosed is relevant and necessary for that assistance.

Policies and Practices for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System—

Storage: Electronic media and file folders for hard-copy records.

Retrievability: By name of individual or other identifying particulars.

Safeguards:

1. *Authorized Users:* A database security package is implemented on CDC's computer systems 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. Guard service in buildings provides personnel screening of visitors. The local fire department is located directly next door to the Clifton Road facility. The computer room is protected by an automatic sprinkler system, numerous automatic sensors (e.g., water, heat, smoke, etc.) are installed, and a proper mix of portable fire extinguishers is located throughout the computer room. Computer files are backed up on a routine basis. Hard-copy records are stored in locked cabinets at CDC headquarters and CDC Quarantine stations which are located in a secure area of the airport.

3. *Procedural Safeguards:* Protection for computerized records, both on the mainframe and the National Center 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 back-up procedures, and secure off-site storage is available. To avoid inadvertent data disclosure, measures are taken to ensure that all data are removed from electronic media containing Privacy Act information. 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.

Implementation Guidelines: The safeguards outlined above are in accordance with the HHS Information Security Program Policy and FIPS Pub 200, "Minimum Security Requirements for Federal Information and Information Systems." Data maintained on CDC's Mainframe and the National Centers' LANs 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.

Retention and Disposal: Contact tracing records will be maintained in the agency until the contact investigation is complete or no longer than twelve months, in accordance with proposed retention schedules; remaining quarantine records would be maintained 10 or 20 years, based on the applicable CDC records control schedule. Disposal methods include wiping electronic media and macerating paper materials.

System Manager(s) and Address(es):

Director, NCPDCID, Coordinating Center for Infectious Diseases, Bldg. 1, Rm. 6013, MS C12, 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 listed 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.

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, private physicians, state and local health departments, other health-care providers, conveyance personnel, cooperating public health agencies, foreign governments including ministries of health, and other federal agencies.

System Exempted from Certain Provisions of the Act: None.

Content created by Freedom of Information Act (FOIA) Division
Content last reviewed December 19, 2017