

training is required and conducted for authorized users regarding proper handling and safeguarding of personally identifiable information. OMH and OMHRC staff are trained on HHS policies regarding personal use of health information technology.

RETENTION AND DISPOSAL:

1. *Mailing List*: Records are maintained until removed by the individual on whom information is maintained or until the individual requests removal.

2. *Resource Persons Network*: Records are maintained for as long as the individual indicates a willingness to serve as a Resource Person by responding affirmatively to update requests.

3. *Training Institute File*: Records are maintained for three years following the end of the specific training course.

4. *Campaign File*: Contact information on individuals is maintained for the duration of the campaign. Resumes are retained for one year.

5. *Organizational Databases*: Records are maintained until the organization about which information is maintained no longer works in minority health, or until the contact person for the organization changes.

6. *Inquiry Tracking System*: Records are maintained for three years following order fulfillment.

Records no longer maintained are disposed of by deletion from electronic media and shredding of hard copy records. Electronic records deleted from active files are maintained in system back-up files on tape media for one year.

SYSTEM MANAGER AND ADDRESS:

Director, Division of Information and Education, Office of Minority Health, 1101 Wootton Parkway, Suite 600, Rockville, MD 20852.

NOTIFICATION PROCEDURE:

To determine whether the system contains a record on you, please write to the system manager at the address above, providing name, address, e-mail, telephone and organizational affiliation.

RECORD ACCESS PROCEDURE:

To determine whether the system contains a record on you, please write to the system manager at the address above, providing name, address, e-mail, telephone and organizational affiliation.

CONTESTING RECORD PROCEDURES:

Contesting Records: Mailing list members may unsubscribe from the mailing list or correct their entry by clicking on a link in an e-mail received from the system. Unsubscribing will remove subscriber information from the

system. For all other deletions and corrections, please write, call, e-mail or fax Office of Minority Health Resource Center, 1101 Wootton Parkway, Suite 650, Rockville, MD 20852, telephone 800-444-6472, e-mail info@omhrc.gov, fax 240-453-2883. The identity of the requestor will be verified by comparison with information contained in the existing record. An individual may request accounting of disclosures outside the department. The right to contest records is limited to information that is incomplete, irrelevant, incorrect, or untimely.

RECORDS SOURCE CATEGORIES:

Information is collected via mail, e-mail, Web form, telephone or in person at conferences and meetings from individuals who receive some type of communication from OMH. Listings in the organizational database are generally drawn from publicly available documents such as directories, newsletters, and organizational Web sites and are confirmed through direct contact with the organization. Names of contact individuals at organizations partnering with OMH on an initiative, project or campaign are provided by the organization.

SYSTEMS EXEMPTED FROM CERTAIN PROVISIONS OF THE ACT:

None.

[FR Doc. 2010-8413 Filed 4-12-10; 8:45 am]

BILLING CODE 4150-29-P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Office for Civil Rights; Privacy Act of 1974, Amended System of Records

AGENCY: Office for Civil Rights (OCR), Department of Health and Human Services (HHS or the Department).

ACTION: Notice of modified or altered System of Records (SOR).

SUMMARY: In accordance with the Privacy Act, we are proposing to modify or alter an existing SOR, "Program Information Management System (PIMS)," System No. 09-90-0052, published at 67 FR 57011, September 6, 2002. First, we propose to add a new authority, the Health Information Technology for Economic and Clinical Health (HITECH) Act, part of the American Recovery and Reinvestment Act of 2009 (Pub. L. 111-5), to those under which OCR collects information. Second, we propose to add three new purposes of the PIMS system. Third, we propose to add six new routine uses to the PIMS system. Fourth, we propose to expand the categories of information

stored in the PIMS system to include information that covered entities under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and their business associates report to the Secretary with respect to a breach of protected health information. See Effective Dates section for comment period.

DATES: *Effective Dates:* OCR filed a system report with the Chair of the House Committee on Government Reform and Oversight, the Chair of the Senate Committee on Homeland Security and Governmental Affairs, and the Administrator, Office of Information and Regulatory Affairs, Office of Management and Budget (OMB) on March 30, 2010. Comments on this SOR may be submitted within 40 days from the publication of the notice, or from the date it was submitted to OMB and the Congress, whichever is later. The SOR, including routine uses, will become effective at the end of the 40-day period, unless OCR receives comments that require alterations to this notice.

ADDRESSES: You may submit comments by any of the following methods (please do not submit duplicate comments):

- *Federal eRulemaking Portal:* <http://www.regulations.gov>. Follow the instructions for submitting comments. Attachments should be in Microsoft Word, WordPerfect, or Excel; however, we prefer Microsoft Word.

- *Regular, Express, or Overnight Mail:* U.S. Department of Health and Human Services, Office for Civil Rights, Attention: PIMS System of Records, Hubert H. Humphrey Building, Room 509F, 200 Independence Avenue, SW., Washington, DC 20201. Please submit one original and two copies.

- *Hand Delivery or Courier:* Office for Civil Rights, Attention: PIMS System of Records, Hubert H. Humphrey Building, Room 509F, 200 Independence Avenue, SW., Washington, DC 20201. Please submit one original and two copies. (Because access to the interior of the Hubert H. Humphrey Building is not readily available to persons without Federal government identification, commenters are encouraged to leave their comments in the mail drop slots located in the main lobby of the building.)

Inspection of Public Comments: All comments received before the close of the comment period will be available for public inspection, including any personally identifiable or confidential business information that is included in a comment. We will post all comments received before the close of the comment period at <http://www.regulations.gov>. Because

comments will be made public, they should not include any sensitive personal information, such as a person's social security number; date of birth; driver's license number, state identification number or foreign country equivalent; passport number; financial account number; or credit or debit card number. Comments also should not include any sensitive health information, such as medical records or other individually identifiable health information.

FOR FURTHER INFORMATION CONTACT: For further information contact: PIMS Project Manager, Management Operations Division, Office for Civil Rights, 200 Independence Ave., SW., Room 509F, Washington, DC 20201. Telephone number: (202) 619-2888.

SUPPLEMENTARY INFORMATION: The system of records (*i.e.*, PIMS) described in the OCR's Privacy Act notice, 67 FR 57011 (Sept. 6, 2002), is used by OCR staff and consists of an electronic repository of information and documents, and supplementary paper document files. PIMS effectively combined and replaced OCR's two previous systems of records, (CIMS and the Complaint File and Log), into a single, integrated system with enhanced electronic storage, retrieval, and tracking capacities that allows OCR to manage more effectively the information that it collects. PIMS was modified to add a new authority, the Patient Safety and Quality Improvement Act of 2005, and altered to add two new routine uses in OCR's Privacy Act notice at 72 FR 8734 (Feb. 27, 2007).

The Privacy Act permits OCR to disclose information or records pertaining to an individual without that individual's consent if the information is to be used for a purpose that is compatible with the purpose(s) for which the information was collected, 5 U.S.C. 552a(b)(3). Any such disclosure is known as a "routine use." The PIMS system conforms to applicable law and policy governing the privacy and security of Federal automated information systems. These include but are not limited to: The Privacy Act of 1974, Federal Information Security Management Act of 2002, Computer Security Act of 1987, the Paperwork Reduction Act of 1995, the Clinger-Cohen Act of 1996, and OMB Circular A-130, Appendix, III, "Security of Federal Automated Information Resources."

OCR has prepared a system security plan as required by OMB Circular A-130, Appendix III. This plan conforms fully to guidance issued by the National Institute for Standards and Technology

(NIST) in NIST Special Publication 800-18, "Guide for Developing Security Plans for Information Technology Systems." The plan includes performance of a risk assessment that addresses the confidentiality and integrity of the data. Only authorized users have access to the information in the system.

Specific access is structured around need and is determined by the person's role in the organization. Access is managed through the use of electronic access control lists, which regulate the ability to read, change, and delete information in the system. Each OCR user has read access to designated information in the system, with the ability to modify only their own submissions or those of others within their region or group. Data identified as confidential is so designated and only specified individuals are granted access. The system maintains an audit trail of all actions against the data base. All electronic data is stored on servers maintained in locked facilities with computerized access control allowing access to only those support personnel with a demonstrated need for access. A database is kept of all individuals granted security card access to the room, and all visitors are escorted while in the room. The server facility has appropriate environmental security controls, including measures to mitigate damage to automated information system resources caused by fire, electricity, water, and inadequate climate controls. Access control to servers, individual computers and databases includes a required user log-on with a password, inactivity lockout to systems based on a specified period of time, legal notices and security warnings at log-on, and remote access security that allows user access for remote users (*e.g.*, while on government travel) under the same terms and conditions as for users within the office. System administrators have appropriate security clearance. Printed materials are filed in secure cabinets in secure Federal buildings with access based on need as described above for the automated component of the PIMS system.

Section 13402(e)(3) of the HITECH Act requires HIPAA covered entities to provide notice to the Secretary of the Department of Health and Human Services (HHS or the Department) of a breach of unsecured protected health information. Notice to the Secretary is required immediately if a breach affects 500 or more individuals and annually for breaches affecting fewer than 500 individuals. Section 13402(e)(4) of the HITECH Act requires the Secretary to

make available to the public on the HHS Web site a list that identifies each covered entity involved in a breach affecting more than 500 individuals. To implement these HITECH provisions, HHS published an interim final rule on August 24, 2009 (74 FR 42740). Section 164.408(a) of the regulations published in the interim final rule requires covered entities to notify the Secretary of breaches of unsecured protected health information. Section 164.408(b) requires breaches that affect 500 or more individuals to be reported to the Secretary contemporaneously with notice to the individual—that is, without unreasonable delay and in no case later than 60 calendar days after a covered entity discovers a breach (subject to a law enforcement delay as provided in section 164.412). Section 164.408(c) sets out the annual reporting for breaches affecting fewer than 500 individuals. Covered entities are required to report these breaches in the manner specified on the HHS Web site. A breach report form that has been approved by OMB for collection of this information can be found at <http://transparency.cit.nih.gov/breach/index.cfm>. A breach report must be filed through this Web site.

Accordingly, this notice modifies PIMS by adding a new authority for maintenance of the system, identifies three new purposes of the PIMS system, adds new routine uses of the PIMS system, and expands the categories of information stored in the PIMS system. In addition to the new routine uses proposed because of breach notification requirements under the HITECH Act, one proposed new routine use regards responding to breaches of personally identifiable information within the Department, consistent with Office of Management and Budget (OMB) Memorandum 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, dated May 22, 2007. Another proposed new routine use regards disclosing relevant personally identifiable information including the identity of covered entities and business associates to obtain information relevant and necessary to investigate violations and potential violations, as well as to conduct compliance reviews, of the Federal laws and regulations OCR has legal authority to enforce. The last new proposed routine use regards allowing OCR to disclose relevant information to the public to inform the public of the results of investigations and compliance reviews of the Federal laws and regulations that OCR has legal authority to enforce, after OCR determines that

the disclosure would not constitute an unwarranted invasion of personal privacy. OCR expects these modifications will not result in any unwarranted invasion of personal privacy.

OCR proposes to add the following authority for maintenance of the PIMS system: section 13402 of the HITECH Act, part of the American Recovery and Reinvestment Act of 2009 (Pub. L. 111-5).

OCR proposes to add the following three new purposes of the PIMS system: (1) To collect, maintain, and post on the HHS Web site a list of covered entities that experience breaches of unsecured protected health information affecting more than 500 individuals using information reported to the Secretary by covered entities (or a business associate on behalf of a covered entity) as required by section 13402(e) of the HITECH Act; (2) to develop an annual report to Congress, as required by section 13402(i) of the HITECH Act, regarding breach notification using information reported to the Secretary by covered entities (or a business associate on behalf of a covered entity) under section 13402(e) of the HITECH Act; and (3) to provide technical assistance, training, and guidance materials regarding breaches of protected health information.

OCR proposes to establish the following six new routine use disclosures of information for PIMS. Each routine use is compatible with a stated purpose of the system.

I. The first new routine use allows OCR to post on its Web site, as required by section 13402(e)(4) of the HITECH Act, information reported by a covered entity (or a business associate on behalf of a covered entity) to the Secretary pursuant to section 13402(e)(3) of the HITECH Act that identifies covered entities that experience breaches of unsecured protected health information affecting more than 500 individuals.

II. The second new routine use allows OCR to disclose information regarding breaches of unsecured protected health information in an annual report to Congress, as required by section 13402(i) of the HITECH Act, regarding the number and nature of the breaches reported to the Secretary and actions taken in response to such breaches.

III. The third new routine use allows OCR to disclose information regarding breaches of unsecured protected health information to the public and to appropriate Federal agencies and Department contractors to provide technical assistance, training, and guidance materials, after OCR determines that the disclosure would

not constitute an unwarranted invasion of personal privacy.

IV. The fourth new routine use allows OCR to disclose information 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 security or confidentiality of information maintained in this system of records, and the information disclosed is relevant and necessary for that assistance.

V. The fifth new routine use allows OCR to disclose information to third party contacts, including public and private organizations, to investigate violations and potential violations, as well as to conduct compliance reviews, of the Federal laws and regulations that OCR has legal authority to enforce.

VI. The sixth new routine use allows OCR to disclose relevant information to the public to inform the public of the results of investigations and compliance reviews of the Federal laws and regulations that OCR has legal authority to enforce, after OCR determines that the disclosure would not constitute an unwarranted invasion of personal privacy.

OCR proposes to add the following category of information included in the PIMS system: Information that HIPAA covered entities (or a business associate on behalf of a covered entity) (defined in 45 CFR 160.103) are required to provide to HHS to fulfill their breach notification requirements to the Secretary pursuant to section 13402(e) of the HITECH Act. This information includes the name, address, and contact information of the covered entity or business associate, as well as the contact name of the individual at the covered entity or business associate that reported the breach of protected health information.

OCR will continue to collect only information that is necessary to perform the PIMS functions. We only disclose the minimum personal data necessary to achieve the purpose of PIMS. Disclosure of information from the system will be approved only to the extent necessary to accomplish the purpose of the disclosure. Further, OCR continues to take precautionary measures to minimize the risks of unauthorized access to the records and the potential harm to individual privacy or other individual rights. In addition, OCR makes disclosures from the PIMS system only with consent of the subject individual, or his/her legal representative, or in accordance with an applicable exception provision of the Privacy Act. OCR, therefore, believes

that no unfavorable effect on individual privacy will result from the modifications and alterations to PIMS proposed herein.

The following notice is written in the present, rather than the future tense, to avoid the unnecessary expenditure of public funds to republish the notice after the system has become effective.

Dated: March 30, 2010.

Georgina C. Verdugo,
Director, Office for Civil Rights.

09-90-0052

SYSTEM NAME:

"Program Information Management System" (PIMS) (09-90-0052) HHS/OS/OCR.

SECURITY CLASSIFICATION:

None.

SYSTEM LOCATION:

The automated portion of the system is maintained at OCR Headquarters. Paper files are maintained in headquarters and regional offices as noted in Appendix I.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Covered individuals include persons who file complaints alleging discrimination or violation of their rights or other violations under the statutes identified below (Authority for Maintenance) and covered entities (*e.g.*, health care providers) that are individuals and not organizations or institutions, investigated by OCR as a result of complaints filed or through reviews conducted by OCR. Covered individuals also include persons who submit correspondence to OCR related to other compliance activities (*e.g.*, outreach and public education), and other correspondence unrelated to a complaint or review and requiring responses by OCR. Covered individuals also include covered entities and business associates (that are individuals and not organizations or institutions), as defined in 45 CFR 160.103, who report breaches of protected health information by submitting a breach report through the HHS Web site. In addition, OCR employees that use the system to record the status of their work are covered by the system.

CATEGORIES OF RECORDS IN THE SYSTEM:

The system encompasses a variety of records having to do with complaints, reviews, correspondence, and reports of breaches of protected health information. For example, the system includes records containing individual names, Social Security numbers (SSN), tax identification numbers (TIN),

addresses, dates of birth, provider names and addresses, physicians' names, prescriber identification numbers, assigned provider numbers (facility, referring/servicing physician), and/or other identification numbers of HIPAA covered entities.

The complaint files and log include complaint allegations, information gathered during the complaint investigation, findings and results of the investigation, and correspondence relating to the investigation, as well as status information for all complaints. This component of PIMS is exempt from the notification, access, correction and amendment provisions of the Privacy Act (*see below: Systems Exempted From Certain Provisions of the Act*). Equivalent types of information are maintained for reviews and correspondence activities—namely, information gathered, findings, results, correspondence and status.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Authority for the collection, maintenance, and disclosures from this system is given under Title VI of the 1964 Civil Rights Act; Sections 533, 542, 794, 855, 1947 and 1908 of the Public Health Service Act; Sections 504 and 508 of the Rehabilitation Act of 1973; Title II of the Americans with Disabilities Act of 1990; the Age Discrimination Act of 1975; the Equal Employment Opportunity Provisions of the Public Telecommunications Financing Act of 1978; Title VI and Title XVI of the Public Health Service Act (the “community services obligation” of facilities funded under the Act); Title IX of the 1972 Education Amendments; Section 407 of the Drug Abuse Office and Treatment Act; Section 321 of the Comprehensive Alcohol Abuse and Alcoholism Prevention, Treatment, and Rehabilitation Act of 1970; Section 508 of the Social Security Act; the Family Violence Prevention and Services Act; Low-Income Home Energy Assistance Act of 1981; Section 1808 of the Small Business Job Protection Act of 1996; the Health Insurance Portability and Accountability Act of 1996; the Patient Safety and Quality Improvement Act of 2005 (Patient Safety Act); and section 13402 of the Health Information Technology for Economic and Clinical Health (HITECH) Act.

PURPOSE(S) OF THE SYSTEM:

PIMS is used by OCR staff and consists of an electronic repository of information and documents, and supplementary paper document files. PIMS effectively combines and replaces OCR's two previous systems of records, the “Case Information Management

System (CIMS), HHS/OS/OCR, 09–90–0050,” and the “Complaint File and Log, HHS/OS/OCR 09–00–0051,” into a single, integrated system with enhanced electronic storage, retrieval and tracking capacities that allows OCR to manage more effectively the information it collects.

The system is designed to allow OCR to integrate all of OCR's various business processes, including all its compliance activities, to allow for real time access and results reporting and other varied information management needs. PIMS provides: (1) A single, central, electronic repository of all significant OCR documents and information, including investigative files, correspondence, administrative records, policy and procedure manuals and other documents and information developed or maintained by OCR; (2) easy, robust capability to search all the information in OCR's repository; (3) better quality control at the front end with simplified data entry and stronger data validation; (4) tools to help staff work on and manage their casework, and (5) supplementary paper document files. The system has the capacity to generate reports concerning the status of all current and closed complaints, reviews, and correspondence; track outreach, training, and other activities; and to locate and retrieve information, and report results, in order to manage more efficiently OCR's work. In addition, PIMS allows for the tracking of work assignments to employees to facilitate workload balancing, timely response to complaints and completion of reviews, and outreach and public education initiatives focused on organizations and individuals.

PIMS also is used by OCR: (1) To collect, maintain, and post on the HHS Web site a list of covered entities that experience breaches of unsecured protected health information affecting more than 500 individuals using information reported to the Secretary by covered entities (or a business associate on behalf of a covered entity) as required by section 13402(e) of the HITECH Act; (2) to develop an annual report to Congress, as required by section 13402(i) of the HITECH Act, regarding breach notification using information reported to the Secretary by covered entities (or a business associate on behalf of a covered entity) pursuant to section 13402(e) of the HITECH Act; and (3) to provide technical assistance, training, and guidance regarding breaches of protected health information.

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

The Privacy Act allows us to disclose information without an individual's consent if the information is to be used for a purpose that is compatible with the purpose(s) for which the information was collected. Any such compatible use of data is known as a “routine use.” The routine uses in this system meet the compatibility requirement of the Privacy Act. The following are the routine use disclosures of information maintained in the PIMS system:

I. The first routine use for this system, permitting disclosure to a congressional office, allows subject individuals to obtain assistance from their representatives in Congress, should they so desire. Such disclosure would be made only pursuant to the request of the individual.

II. The second routine use allows disclosure to the Department of Justice or a court in the event of litigation.

III. The third routine use allows referral to the appropriate agency, 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.

IV. The fourth routine use allows disclosure of records to contractors for the purpose of processing or refining records in the system.

V. The fifth routine use allows records to be disclosed to student volunteers, individuals working under a personal services contract, and other individuals performing functions for the Department but technically not having the status of agency employees, if they need access to the records in order to perform their assigned agency functions.

VI. The sixth routine use allows referrals of Age Discrimination Act complaints to the Federal Mediation and Conciliation Service (FMCS) for purposes of mediation.

VII. The seventh routine use allows OCR to post on its Web site, as required by section 13402(e)(4) of the HITECH Act, information reported by a covered entity (or a business associate on behalf of a covered entity) to the Secretary pursuant to section 13402(e)(3) of the HITECH Act that identifies covered entities that experience breaches of unsecured protected health information affecting more than 500 individuals.

VIII. The eighth routine use allows OCR to disclose information regarding breaches of unsecured protected health information in an annual report to Congress, as required by section 13402(i) of the HITECH Act, regarding the number and nature of the breaches

reported to the Secretary and actions taken in response to such breaches.

IX. The ninth routine use allows OCR to disclose information regarding breaches of unsecured protected health information to the public and to appropriate Federal agencies and Department contractors to provide technical assistance, training, and guidance materials, after OCR determines that the disclosure would not constitute an unwarranted invasion of personal privacy.

X. The tenth routine use allows OCR to disclose information 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 security or confidentiality of information maintained in this system of records, and the information disclosed is relevant and necessary for that assistance.

XI. The eleventh routine use allows OCR to disclose information to third party contacts, including public and private organizations, to investigate violations and potential violations, as well as to conduct compliance reviews, of the Federal laws and regulations that OCR has legal authority to enforce.

XII. The twelfth routine use allows OCR to disclose relevant information to the public to inform the public of the results of investigations and compliance reviews of the Federal laws and regulations that OCR has legal authority to enforce, after OCR determines that the disclosure would not constitute an unwarranted invasion of personal privacy.

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

STORAGE:

Automated records are maintained on magnetic disc and tape back-up. Paper records are kept in file folders.

RETRIEVABILITY:

Records are indexed by transaction number, but may be retrieved by name, street address, and other complainant, covered entity, or business associate characteristic (such as type of entity, city, state, and type of service provided).

SAFEGUARDS:

The PIMS system conforms to applicable law and policy governing the privacy and security of Federal automated information systems. These include but are not limited to: the Privacy Act of 1974, Federal Information Security Management Act of 2002, Computer Security Act of 1987,

the Paperwork Reduction Act of 1995, the Clinger-Cohen Act of 1996, and OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources." OCR has prepared a system security plan as required by OMB Circular A-130, Appendix III. This plan conforms fully to guidance issued by the National Institute for Standards and Technology (NIST) in NIST Special Publication 800-18, "Guide for Developing Security Plans for Information Technology Systems." The plan includes conduct of a risk assessment that addresses the confidentiality and integrity of the data. Only authorized users have access to the information in the system. Categories of users include: OCR investigators, regional and headquarters managers, team leaders, OCR budget and Government Performance and Results Act planning staff, program and policy staff, and data analysts. Specific access is structured around need and is determined by the person's role in the organization. Access is managed through the use of electronic access control lists, which regulate the ability to read, change, and delete information in the system. Each OCR user has read access to designated information in the system, with the ability to modify only their own submissions or those of others within their region or group. Data identified as confidential is so designated and only specified individuals are granted access. The system maintains an audit trail of all actions against the data base.

All electronic data is stored on servers maintained in locked facilities with computerized access control allowing access to only those support personnel with a demonstrated need for access. A database is kept of all individuals granted security card access to the room, and all visitors are escorted while in the room. The server facility has appropriate environmental security controls, including measures to mitigate damage to automated information system resources caused by fire, electricity, water, and inadequate climate controls.

Access control to servers, individual computers, and databases includes a required user log-on with a password, inactivity lockout to systems based on a specified period of time, legal notices and security warnings at log-on, and remote access security that allows user access for remote users (e.g., while on government travel) under the same terms and conditions as for users within the office. System administrators have appropriate security clearance. Printed materials are filed in secure cabinets in secure Federal buildings with access

based on need as described above for the automated component of the PIMS system.

RETENTION AND DISPOSAL:

Documents related to breaches are retained at OCR for two years from the date the breach is reported and then are archived at the National Archives and Records Administration for 15 years. Correspondence is retained for one year following the end of the fiscal year in which processed.

SYSTEM MANAGER AND ADDRESS:

PIMS Project Manager, Management Operations Division, Office for Civil Rights, 200 Independence Ave., SW., Room 509F, Washington, DC 20201.

NOTIFICATION PROCEDURE:

Contact System Manager (above). Include name and address of complainant, and name of the recipient against which the allegation was filed. The Department is exempting all investigative records from this provision (see below: Records Exempted).

RECORD ACCESS PROCEDURE:

Same as notification procedures. Requesters also should reasonably specify the record contents being sought. Requests should be made to the system manager (above). The Department is exempting all investigative records from this provision. (See below: Records Exempted).

CONTESTING RECORD PROCEDURE:

Contact the official(s) at the address specified under System Manager, and reasonably identify the record and specify the information to be contested and corrective action sought with supporting justification. (These procedures are in accordance with Department Regulations (45 CFR 5b.7) The Department is exempting all investigative records from this provision (see below: Records Exempted).

RECORD SOURCE CATEGORIES:

Information is provided by complainants, covered entities, and business associates.

SYSTEM RECORDS EXEMPTED FROM CERTAIN PROVISIONS OF THE ACT:

OCR investigative records maintained in PIMS, either as paper records or electronic documents, are records compiled for law enforcement purposes and are exempt under subsection (k)(2) from the notification, access, correction, and amendment provisions of the Privacy Act.

APPENDIX NUMBER 1—SYSTEM LOCATIONS:

This system is located at HHS offices in the following cities:

Headquarters, PIMS Project Manager, Management Operations Division, Office for Civil Rights, 200 Independence Ave., SW., Room 509F, Washington, DC 20201.

Region I, Regional Manager, OCR/HHS, J.F. Kennedy Federal Building—Room 1875 Boston, MA 02203.

Region II, Regional Manager, OCR/HHS, 26 Federal Plaza—Suite 3312, New York, NY 10278.

Region III, Regional Manager, OCR/HHS, 150 S. Independence Mall West, Suite 372, Public Ledger Building, Philadelphia, PA 19106–9111.

Region IV, Regional Manager, OCR/HHS, Atlanta Federal Center, Suite 3B70, 61 Forsyth Street, SW., Atlanta, GA 30303–8909.

Region V, Regional Manager, OCR/HHS, 233 N. Michigan Ave, Suite 240, Chicago, IL 60601.

Region VI, Regional Manager, OCR/HHS, 1301 Young Street, Suite 1169, Dallas, TX 75202.

Region VII, Regional Manager, OCR/HHS, 601 E. 12th Street—Room 248, Kansas City, MO 64106.

Region VIII, Regional Manager, OCR/HHS, Federal Office Building, 1961 Stout Street—Room 1426 FOB, Denver, CO 80294–3538.

Region IX, Regional Manager, OCR/HHS, 90 7th Street, Suite 4–100, San Francisco, CA 94103.

Region X, Regional Manager, OCR/HHS, 2201 Sixth Avenue— M/S: RX–11, Seattle, WA 98121–2290.

[FR Doc. 2010–8412 Filed 4–12–10; 8:45 am]

BILLING CODE 4153–01–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Centers for Disease Control and Prevention

[30Day–10–0739]

Agency Forms Undergoing Paperwork Reduction Act Review

The Centers for Disease Control and Prevention (CDC) publishes a list of information collection requests under review by the Office of Management and Budget (OMB) in compliance with the Paperwork Reduction Act (44 U.S.C. Chapter 35). To request a copy of these requests, call the CDC Reports Clearance Officer at (404) 639–5960 or send an e-mail to omb@cdc.gov. Send written comments to CDC Desk Officer, Office of Management and Budget, Washington, DC or by fax to (202) 395–5806. Written comments should be received within 30 days of this notice.

Proposed Project

CDC Oral Health Management Information System (OMB no. 0920–0739, exp. 6/30/2010)—Revision—Division of Oral Health, National Center for Chronic Disease Prevention and Health Promotion (NCCDPHP), Centers for Disease Control and Prevention (CDC).

Background and Brief Description

The CDC seeks to improve the oral health of the nation by targeting efforts to improve the infrastructure of state and territorial oral health departments, developing effective programs to improve the oral health of children and adults, and reducing health disparities among high-risk groups. Through a

cooperative agreement program, CDC provides funding to oral health programs in states and territories.

The CDC collects information from awardees to support oral health program management, consulting and evaluation. The information collection is supported by an electronic management information system (MIS) known as the Management Overview for Logistics, Analysis, and Reporting (MOLAR) system. The MIS provides a centralized, standardized and searchable repository of information about each awardee’s objectives, programmatic activities, performance indicators, and financial status.

CDC requests OMB approval to continue the electronic collection of information for three years. The information collected will continue to facilitate CDC’s ability to monitor, evaluate, and compare individual programs; provide technical assistance to states and territories; share and disseminate lessons learned; assess and report aggregate information regarding the overall effectiveness of oral health infrastructure and capacity at the state and territorial level; and monitor national progress toward meeting *Healthy People* goals.

Information will be collected electronically twice per year. No changes to the MIS or the estimated burden per response are proposed. There is an increase in the total estimated annualized burden due to an increase in the number of CDC-funded oral health programs. There are no costs to respondents other than their time. The total estimated annualized burden hours are 462.

ESTIMATED ANNUALIZED BURDEN HOURS

Type of respondents	Number of respondents	Number of responses per respondent	Average burden per response (in hours)
State Oral Health Programs	21	2	11

Dated: April 6, 2010.

Maryam I. Daneshvar,

Acting Reports Clearance Officer, Centers for Disease Control and Prevention.

[FR Doc. 2010–8441 Filed 4–12–10; 8:45 am]

BILLING CODE 4163–18–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Administration for Children and Families

Agency Recordkeeping/Reporting Requirements Under Emergency Review by the Office of Management and Budget (OMB)

Title: Strengthening Communities Fund Program Evaluation.

OMB No.: New Collection.

Description: This proposed information collection activity is to obtain evaluation information from Strengthening Communities Fund (SCF) grantees. Grantees include participants in two SCF grant programs contributing to the economic recovery as authorized in the American Recovery and Reinvestment Act of 2009 (ARRA). The SCF evaluation is an important opportunity to examine the outcomes achieved by the Strengthening Communities Fund in meeting its