

budget period. The progress report will serve as your non-competing continuation application, and must contain the following elements:

- a. Current Budget Period Activities Objectives.
  - b. Current Budget Period Financial Progress.
  - c. New Budget Period Program Proposed Activity Objectives.
  - d. Budget.
  - e. Measures of Effectiveness.
  - f. Additional Requested Information.
2. Annual progress report, due 90 days after the end of the budget period.
  3. Financial status report, no more than 90 days after the end of the budget period.
  4. Final financial and performance reports, no more than 90 days after the end of the project period.

#### VII. Agency Contacts

We encourage inquiries concerning this announcement. For general questions, contact: Technical Information Management Section, CDC Procurement and Grants Office, 2920 Brandywine Road, Atlanta, GA 30341, Telephone: 770-488-2700.

For program technical assistance, contact: Debra Hayes-Hughes, Project Officer, Centers for Disease Control and Prevention, 1600 Clifton Road, NE., MS E-47, Atlanta, GA 30333, Telephone: 404-639-4493, E-mail: [DHayes-Hughes@cdc.gov](mailto:DHayes-Hughes@cdc.gov).

For financial, grants management, or budget assistance, contact: Kang Lee, Grants Management Specialist, CDC Procurement and Grants Office, 2920 Brandywine Road, Atlanta, GA 30341, Telephone: 404-498-1917, E-mail: [kil8@cdc.gov](mailto:kil8@cdc.gov).

#### VIII. Other Information

This and other CDC funding opportunity announcements can be found at <http://www.cdc.gov>. Click on "Funding," then "Grants and Cooperative Agreements."

Dated: June 28, 2005.

#### Alan A. Kotch,

Acting Deputy Director, Procurement and Grants Office, Centers for Disease Control and Prevention.

[FR Doc. 05-13223 Filed 7-5-05; 8:45 am]

BILLING CODE 4163-18-P

## DEPARTMENT OF HEALTH AND HUMAN SERVICES

### Centers for Medicare & Medicaid Services

#### Privacy Act of 1974; Report of a New System of Records

**AGENCY:** Department of Health and Human Services (HHS), Centers for Medicare & Medicaid Services (CMS).

**ACTION:** Notice of a new System of Records (SOR).

**SUMMARY:** In accordance with the requirements of the Privacy Act of 1974, we are proposing to establish a new system of records titled, "Health Insurance Portability and Accountability Act (HIPAA) Information Tracking System (HITS), System No. 09-70-0544." The Office of E-Health Standards and Services (OESS) has been delegated the responsibility to regulate and enforce compliance for violations of Transactions and Code Sets, Security, and Unique Identifier provisions of HIPAA. Enforcement of these provisions is a complaint driven process; seeking voluntary compliance from all HIPAA covered entities. OESS has procured the services of a contractor to provide a database for complaint intake and management, to manage and maintain the overall electronic complaint process. Due to investigatory activities, CMS is exempting this system from the notification, access, correction and amendment provisions of the Privacy Act of 1974.

The purpose of this system is to store the results of all OESS regional investigations, to determine if there were violations as charged in the original complaint, to investigate complaints that appear to be in violation of the Transactions and Code Sets, Security, and Unique Identifier provisions of HIPAA, to refer violations to law enforcement activities as necessary, and to maintain and retrieve records of the results of the complaint investigations. Information retrieved from this SOR will also be disclosed to: (1) Support regulatory, reimbursement, and policy functions performed within the agency, HIPAA entities, or by a contractor or consultant; (2) assist another Federal or state agency in the enforcement of HIPAA regulations where sharing the information is necessary to complete the processing of a complaint, contribute to the accuracy of CMS's proper payment of Medicare benefits, and/or enable such agency to administer a Federal health benefits program; (3) support constituent requests made to a congressional

representative; (4) support litigation involving the agency; and (5) combat fraud and abuse in certain health benefits programs. We have provided background information about the modified system in the "Supplementary Information" section below. Although the Privacy Act requires only that CMS provide an opportunity for interested persons to comment on the proposed routine uses, CMS invites comments on all portions of this notice. See "Effective Dates" section for comment period.

**DATES:** *Effective Date:* CMS filed a new SOR report with the Chair of the house Committee on Government Reform and Oversight, the Chair of the Senate Committee on Governmental Affairs, and the Administrator, Office of Information and Regulatory Affairs, Office of Management and Budget (OMB) on June 28, 2005. We will not disclose any information under a routine use until 30 days after publication. We may defer implementation of this SOR or one or more of the routine use statements listed below if we receive comments that persuade us to defer implementation.

**ADDRESSES:** The public should address comment to the CMS Privacy Officer, Mail-stop N2-04-27, 7500 Security Boulevard, Baltimore, Maryland 21244-1850. Comments received will be available for review at this location, by appointment, during regular business hours, Monday through Friday from 9 a.m.-3 p.m., eastern daylight time.

**FOR FURTHER INFORMATION CONTACT:** Michael Phillips, Health Insurance Specialist, OESS, CMS, 7500 Security Boulevard, Mail Stop S2-24-15, Baltimore, Maryland 21244-1849, Telephone Number (410) 786-6713, [mphillips@cms.hhs.gov](mailto:mphillips@cms.hhs.gov).

**SUPPLEMENTARY INFORMATION:** HITS is used by OESS staff and consists of an electronic repository of information and documents and supplementary paper document files. The HITS system allows OESS to integrate all of OESS' various business process including all of its investigation activities to allow real time access and results reporting and other varied information management needs. HITS provides (1) a single, central, electronic repository of all OHS complaint documents and information including investigative files, correspondence, and administrative records; (2) easy, robust capability to search all of the information in OESS' 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) includes supplementary paper files. The system

has the capacity to generate reports concerning the status of current and closed complaints, reviews and correspondence.

OESS investigative files maintained in HITS are either received as electronic documents or paper records that are compiled for law enforcement purposes. In the course of investigations, OESS often has a need to obtain confidential information involving individuals other than the complainant. In these cases, it is necessary for OHS to: (1) Preserve the confidentiality of this information, (2) avoid unwarranted invasions of personal privacy, and (3) assure recipients of Federal financial assistance that such information provided to OESS will be kept confidential. This assurance facilitates prompt and effective completion of the investigations.

Unrestricted disclosure of confidential information in OESS files can impede ongoing investigations, invade personal privacy of individuals and organizations, reveal the identities of confidential sources, or otherwise impair the ability of OESS to conduct investigations. For these reasons, the CMS is exempting all investigative files from the notification, access, correction and amendment provisions under subsection (k)(2) of the Privacy Act.

## **I. Description of the Proposed System of Records**

### *A. Statutory and Regulatory Basis for SOR*

Authority for maintenance of this system is given under provisions of the Health Insurance Portability and Accountability Act of 1996, Public Law (Pub. L. 104-191), published at 68 FR 60694 (October 23, 2003). These regulations are codified at 45 Code of Federal Regulation, parts 160, 162, and 164.

### *B. Collection and Maintenance of Data in the System*

HITS will maintain a file of complaint allegations, information gathered during the complaint investigation, findings, and results of the investigation, and correspondence relating to the investigation. The collected information will contain name, address, telephone number, health insurance claim (HIC) number, geographic location, as well as, background information relating to Medicare or Medicaid issues of the complainant.

## **II. Agency Policies, Procedures, and Restrictions on the Routine Use**

### *A. Agency Policies, Procedures, and Restrictions on the Routine Use*

The Privacy Act permits 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 disclosure of data is known as a "routine use." The government will only release HITS information that can be associated with an individual as provided for under "Section III. Proposed Routine Use Disclosures of Data in the System." Both identifiable and non-identifiable data may be disclosed under a routine use.

We will only collect the minimum personal data necessary to achieve the purpose of HITS. CMS has the following policies and procedures concerning disclosures of information that will be maintained in the system. Disclosure of information from the SOR will be approved only to the extent necessary to accomplish the purpose of the disclosure and only after CMS:

1. Determines that the use or disclosure is consistent with the reason that the data is being collected, *e.g.*, to store the results of all OESS regional investigations, to determine if there were violations as charged in the original complaint, to investigate complaints that appear to be in violation of the HIPAA, to refer violations to law enforcement activities as necessary, and to maintain and retrieve records of the results of the complaint investigations.

2. Determines that:
  - a. The purpose for which the disclosure is to be made can only be accomplished if the record is provided in individually identifiable form;
  - b. The purpose for which the disclosure is to be made is of sufficient importance to warrant the effect and/or risk on the privacy of the individual that additional exposure of the record might bring; and
  - c. There is a strong probability that the proposed use of the data would in fact accomplish the stated purpose(s).

3. Requires the information recipient to:
  - a. Establish administrative, technical, and physical safeguards to prevent unauthorized use of disclosure of the record;
  - b. Remove or destroy at the earliest time all patient-identifiable information; and
  - c. Agree to not use or disclose the information for any purpose other than the stated purpose under which the information was disclosed.

4. Determines that the data are valid and reliable.

## **III. Proposed Routine Use Disclosures of Data in the System**

A. 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 proposed routine uses in this system meet the compatibility requirement of the Privacy Act. We are proposing to establish the following routine use disclosures of information maintained in the system:

1. To agency contractors or consultant who have been engaged by the agency to assist in the performance of a service related to this system of records and who need to have access to the records in order to perform the activity.

We contemplate disclosing information under this routine use only in situations in which CMS may enter into a contractual or similar agreement with a third party to assist in accomplishing CMS function relating to purposes for this system or records.

CMS occasionally contracts out certain of its functions when doing so would contribute to effective and efficient operations. CMS must be able to give a contractor or consultant whatever information is necessary for the contractor or consultant to fulfill its duties. In these situations, safeguards are provided in the contract prohibiting the contractor or consultant from using or disclosing the information for any purpose other than that described in the contract and requires the contractor or consultant to return or destroy all information at the completion of the contract.

2. To another Federal or state agency to:

- a. Assist in the enforcement of HIPAA regulations for violations of Transactions and Code Sets, Security, and Unique Identifiers where sharing the information is necessary to complete the processing of a complaint,

- b. Contribute to the accuracy of CMS's proper payment of Medicare benefits, and/or

- c. Enable such agency to administer a Federal health benefits program, or as necessary to enable such agency to fulfill a requirement of a Federal statute or regulation that implements a health benefits program funded in whole or in part with Federal funds.

Other Federal or state agencies in their administration of a Federal health program may require HITS information in order to investigate complaint

allegations, evaluate information gathered during the complaint investigation, review findings and results of the investigation relating to the enforcement of HIPAA regulations for violations of Transactions and Code Sets, Security, and Unique Identifiers.

3. To a member of Congress or to a congressional staff member in response to an inquiry of the congressional office made at the written request of the constituent about whom the record is maintained.

Beneficiaries sometimes request the help of a member of Congress in resolving an issue relating to a matter before CMS. The member of Congress then writes CMS, and CMS must be able to give sufficient information to be responsive to the inquiry.

4. To the Department of Justice (DOJ), court or adjudicatory body when:

a. The agency or any component thereof, or

b. Any employee of the agency in his or her official capacity, or

c. Any employee of the agency in his or her individual capacity where the DOJ has agreed to represent the employee, or

d. The United States Government is a party to litigation or has an interest in such litigation, and by careful review, CMS determines that the records are both relevant and necessary to the litigation and that the use of such records by the DOJ, court or adjudicatory body is compatible with the purpose for which the agency collected the records.

Whenever CMS is involved in litigation, and occasionally when another party is involved in litigation and CMS' policies or operations could be affected by the outcome of the litigation, CMS would be able to disclose information to the DOJ, court or adjudicatory body involved.

5. To a CMS contractor (including, but not necessarily limited to fiscal intermediaries and carriers) that assists in the administration of a CMS-administered health benefits program, or to a grantee of a CMS-administered grant program, when disclosure is deemed reasonably necessary by CMS to prevent, deter, discover, detect, investigate, examine, prosecute, sue with respect to, defend against, correct, remedy, or otherwise combat fraud or abuse in such program.

We contemplate disclosing information under this routine use only in situations in which CMS may enter into a contractual relationship or grant with a third party to assist in accomplishing CMS functions relating to the purpose of combating fraud and abuse.

CMS occasionally contracts out certain of its functions and makes grants when doing so would contribute to effective and efficient operations. CMS must be able to give a contractor or grantee whatever information is necessary for the contractor or grantee to fulfill its duties. In these situations, safeguards are provided in the contract prohibiting the contractor or grantee from using or disclosing the information for any purpose other than that described in the contract and requiring the contractor or grantee to return or destroy all information.

6. To another Federal agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States (including any State or local governmental agency), that administers, or that has the authority to investigate potential fraud or abuse in, a health benefits program funded in whole or in part by Federal funds, when disclosure is deemed reasonably necessary by CMS to prevent, deter, discover, detect, investigate, examine, prosecute, sue with respect to, defend against, correct, remedy, or otherwise combat fraud or abuse in such programs.

Other agencies may require HITS information for the purpose of combating fraud and abuse in such Federally funded programs.

B. Additional Provisions Affecting Routine Use Disclosures. This system contains Protected Health Information (PHI) as defined by HHS regulation "Standards for Privacy of Individually Identifiable Health Information" (45 CFR Parts 160 and 164, 65 FR 82462 (12-28-00), Subparts A and E. Disclosures of PHI authorized by these routine uses may only be made if, and as, permitted or required by the "Standards for Privacy of Individually Identifiable Health Information."

In addition, our policy will be to prohibit release even of not directly identifiable information, except pursuant to one of the routine uses or if required by law, if we determine there is a possibility that an individual can be identified through implicit deduction based on small cell sizes (instances where the patient population is so small that individuals who are familiar with the enrollees could, because of the small size, use this information to deduce the identity of the beneficiary).

#### IV. Safeguards

CMS has safeguards in place for authorized users and monitors such users to ensure against excessive or unauthorized use. Personnel having access to the system have been trained in the Privacy Act and information security requirements. Employees who

maintain records in this system are instructed not to release data until the intended recipient agrees to implement appropriate management, operational and technical safeguards sufficient to protect the confidentiality, integrity and availability of the information and information systems and to prevent unauthorized access.

This system will conform to all applicable Federal laws and regulations and Federal, HHS, and CMS policies and standards as they relate to information security and data privacy. These laws and regulations include but are not limited to: the Privacy Act of 1974; the Federal Information Security Management Act of 2002; the Computer Fraud and Abuse Act of 1986; the Health Insurance Portability and Accountability Act of 1996; the E-Government Act of 2002, the Clinger-Cohen Act of 1996; the Medicare Modernization Act of 2003, and the corresponding implementing regulations. OMB Circular A-130, Management of Federal Resources, Appendix III, Security of Federal Automated Information Resources also applies. Federal, HHS, and CMS policies and standards include but are not limited to: All pertinent NIST publications; the DHHS Information Security Program Handbook and the CMS Information Security Handbook.

#### V. Effects of the Proposed System of Records on Individual Rights

CMS proposes to establish this system in accordance with the principles and requirements of the Privacy Act and will collect, use, and disseminate information only as prescribed therein. Data in this system will be subject to the authorized releases in accordance with the routine uses identified in this system of records.

CMS will take precautionary measures (see item IV above) to minimize the risks of unauthorized access to the records and the potential harm to individual privacy or other personal or property rights of patients whose data are maintained in the system. CMS will collect only that information necessary to perform the system's functions. In addition, CMS will make disclosure from the proposed 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. CMS, therefore, does not anticipate an unfavorable effect on

individual privacy as a result of information relating to individuals.

**John R. Dyer,**  
Chief Operating Officer.

**SYSTEM NO. 09-70-0544**

**SYSTEM NAME:**

“Health Insurance Portability and Accountability Act (HIPAA) Information Tracking System (HITS), HHS/CMS/OESS”.

**SECURITY CLASSIFICATION:**

Level Three Privacy Act Sensitive Data.

**SYSTEM LOCATION:**

Atlantic Telephone & Telegraph Company, Ashburn, Virginia facility under the control of the Center for Medicare & Medicaid Services.

**CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:**

Individuals who have filed complaints alleging violations of the Transactions and Code Sets, Security, and Unique Identifier provisions under the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, 68 FR 60694 (October 23, 2003). These regulations are codified at 45 CFR, parts 160, 162 and 164.

**CATEGORIES OF RECORDS IN THE SYSTEM:**

HITS will maintain a file of complaint allegations, information gathered during the complaint investigation, findings, and results of the investigation, and correspondence relating to the investigation. The collected information will contain name, address, telephone number, health insurance claim (HIC) number, geographic location, as well as, background information relating to Medicare or Medicaid issues.

**AUTHORITY FOR MAINTENANCE OF THE SYSTEM:**

Authority for maintenance of this system is given under provisions of the Health Insurance Portability and Accountability Act of 1996, (Pub. L. 104-191), published at 68 FR 60694 (October 23, 2003). These regulations are codified at 45 Code of Federal Regulation, parts 160, 162, and 164.

**PURPOSE(S) OF THE SYSTEM:**

The purpose of this system is to store the results of all OESS regional investigations, to determine if there were violations as charged in the original complaint, to investigate complaints that appear to be in violation of the Transactions and Code Sets, Security, and Unique Identifier provisions of HIPAA, to refer violations to law enforcement activities as necessary, and to maintain and retrieve

records of the results of the complaint investigations. Information retrieved from this SOR will also be disclosed to: (1) Support regulatory, reimbursement, and policy functions performed within the agency, HIPAA entities, or by a contractor or consultant; (2) assist another Federal or state agency in the enforcement of HIPAA regulations where sharing the information is necessary to complete the processing of a complaint, contribute to the accuracy of CMS's proper payment of Medicare benefits, and/or enable such agency to administer a Federal health benefits program; (3) support constituent requests made to a congressional representative; (4) support litigation involving the agency; and (5) combat fraud and abuse in certain health benefits programs.

**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.” We are proposing to establish the following routine use disclosures of information maintained in the system. Information will be disclosed:

1. To agency contractors or consultants who have been engaged by the agency to assist in the performance of a service related to this system of records and who need to have access to the records in order to perform the activity.
2. To another Federal or state agency to:
  - a. Assist in the enforcement of HIPAA regulations for violations of Transactions and Code Sets, Security, and Unique Identifiers where sharing the information is necessary to complete the processing of a complaint,
  - b. Contribute to the accuracy of CMS's proper payment of Medicare benefits, and/or
  - c. Enable such agency to administer a Federal health benefits program, or as necessary to enable such agency to fulfill a requirement of a Federal statute or regulation that implements a health benefits program funded in whole or in part with Federal funds.
3. To a member of congress or to a congressional staff member in response to an inquiry of the congressional office made at the written request of the constituent about whom the record is maintained.
4. To the Department of Justice (DOJ), court or adjudicatory body when:

a. The agency or any component thereof, or

b. Any employee of the agency in his or her official capacity, or

c. Any employee of the agency in his or her individual capacity where the DOJ has agreed to The United States Government is a party to litigation or has an interest in such litigation, and by careful review, CMS determines that the records are both relevant and necessary to the litigation and that the use of such records by the DOJ, court or adjudicatory body is compatible with the purpose for which the agency collected the records.

5. To a CMS contractor (including, but not necessarily limited to fiscal intermediaries and carriers) that assists in the administration of a CMS-administered health benefits program, or to a grantee of a CMS-administered grant program, when disclosure is deemed reasonably necessary by CMS to prevent, deter, discover, detect, investigate, examine, prosecute, sue with respect to, defend against, correct, remedy, or otherwise combat fraud or abuse in such program.

6. To another Federal agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States (including any State or local governmental agency), that administers, or that has the authority to investigate potential fraud or abuse in, a health benefits program funded in whole or in part by Federal funds, when disclosure is deemed reasonably necessary by CMS to prevent, deter, discover, detect, investigate, examine, prosecute, sue with respect to, defend against, correct, remedy, or otherwise combat fraud or abuse in such programs.

**B. Additional Provisions Affecting Routine Use Disclosures** This system contains Protected Health Information as defined by HHS regulation “Standards for Privacy of Individually Identifiable Health Information” (45 CFR Parts 160 and 164, 65 FR 82462 (12-28-00), Subparts A and E). Disclosures of Protected Health Information authorized by these routine uses may only be made if, and as, permitted or required by the “Standards for Privacy of Individually Identifiable Health Information.”

In addition, our policy will be to prohibit release even of not directly identifiable information, except pursuant to one of the routine uses or if required by law, if we determine there is a possibility that an individual can be identified through implicit deduction based on small cell sizes (instances where the complaint population is so small that individuals who are familiar with the complainants could, because of

the small size, use this information to deduce the identity of the complainant).

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

**STORAGE:**

All records are stored electronically.

**RETRIEVABILITY:**

The complaint data are retrieved by an individual identifier i.e., name of complainant.

**SAFEGUARDS:**

CMS has safeguards in place for authorized users and monitors such users to ensure against excessive or unauthorized use. Personnel having access to the system have been trained in the Privacy Act and information security requirements. Employees who maintain records in this system are instructed not to release data until the intended recipient agrees to implement appropriate management, operational and technical safeguards sufficient to protect the confidentiality, integrity and availability of the information and information systems and to prevent unauthorized access.

This system will conform to all applicable Federal laws and regulations and Federal, HHS, and CMS policies and standards as they relate to information security and data privacy. These laws and regulations include but are not limited to: The Privacy Act of 1974; the Federal Information Security Management Act of 2002; the Computer Fraud and Abuse Act of 1986; the Health Insurance Portability and Accountability Act of 1996; the E-Government Act of 2002; the Clinger-Cohen Act of 1996; the Medicare Modernization Act of 2003, and the corresponding implementing regulations. OMB Circular A-130, Management of Federal Resources, Appendix III, Security of Federal Automated Information Resources also applies. Federal, HHS, and CMS policies and standards include but are not limited to: All pertinent NIST publications; the DHHS Information Security Program Handbook and the CMS Information Security Handbook.

**RETENTION AND DISPOSAL:**

CMS will retain complaint information for a total period not to exceed 25 years.

**SYSTEM MANAGER AND ADDRESS:**

Director, Office of E-Health Standards and Services, CMS, Room S2-26-17, 7500 Security Boulevard, Baltimore, Maryland 21244-1850.

**NOTIFICATION PROCEDURE:**

Exempt. However, portions of this system notice are non-exempt and consideration will be given to requests addressed to the system manager for those portions. For general inquiries, it would be helpful if the request included the system name, address, age, sex, and for verification purposes, the subject individual's name (woman's maiden name, if applicable) and complaint tracking ID number.

**RECORD ACCESS PROCEDURE:**

Same as notification procedures. Requestors should also specify the record contents being sought.

**CONTESTING RECORDS PROCEDURES:**

The subject individual should contact the system manager named above and reasonably identify the records and specify the information to be contested. State the corrective action sought and the reasons for the correction with supporting justification. (These Procedures are in accordance with Department regulation 45 CFR 5b.7).

**RECORDS SOURCE CATEGORIES:**

OESS investigative files maintained in HITS are either received as electronic documents or paper records that are compiled for law enforcement purposes. In the course of investigations, OESS often has a need to obtain confidential information involving individuals other than the complainant.

**SYSTEMS EXEMPTED FROM CERTAIN PROVISIONS OF THE ACT:**

HHS claims exemption of certain records (case files on active fraud investigations) in the system from notification and access procedures under 5 U.S.C. 552a(k)(2) inasmuch as these records are investigatory materials compiled for program (law) enforcement in anticipation of a criminal or administrative proceedings. (See Department Regulation (45 CFR 5b.11)).

[FR Doc. 05-13188 Filed 7-5-05; 8:45 am]

**BILLING CODE 4120-03-P**

**DEPARTMENT OF HEALTH AND HUMAN SERVICES**

**Administration for Children and Families**

**Administration on Children, Youth and Families, Children's Bureau**

*Funding Opportunity Title:* Developing Adoption Services and Supports for Youth Who Wish to Retain Contact with Family Members in Order to Improve Permanency Outcomes.

*Announcement Type:* Initial.

*Funding Opportunity Number:* HHS-2005-ACF-ACYF-CO-0051.

*CFDA Number:* 93.652.

*Due Date for Applications:*

Application is due August 10, 2005.

*Category of Funding Activity:* Social Services and Income Security.

**Executive Summary**

The purposes of funding these demonstration projects are to: (1) Demonstrate the effective implementation of strategies for introducing the concept of open adoption to youth and/or sibling groups who prefer to maintain contact with birth families and/or siblings; (2) demonstrate effective implementation strategies for connecting youth to adults to promote a range of permanency options, particularly adoption and open adoption, and including guardianship and kinship care; (3) demonstrate the effective models of youth leadership and collaboration between youth, siblings and other family members, caseworkers and possible adoptive families in planning for youth permanency; (4) evaluate the processes and outcomes of these strategies and models; and (5) disseminate information about these strategies and models so that other States/locales seeking to implement effective open adoption programs for youth and sibling groups have a demonstrated resource for guidance, insight, and possible replication.

*Priority Area 1*

**I. Funding Opportunity Description**

The purposes of funding these demonstration projects are to: (1) Demonstrate the effective implementation of strategies for introducing the concept of open adoption to youth and/or sibling groups who prefer to maintain contact with birth families and/or siblings; (2) demonstrate effective implementation strategies for connecting youth to adults to promote a range of permanency options, particularly adoption and open adoption, and including guardianship and kinship care; (3) demonstrate the effective models of youth leadership and collaboration between youth, siblings and other family members, caseworkers and possible adoptive families in planning for youth permanency; (4) evaluate the processes and outcomes of these strategies and models; and (5) disseminate information about these strategies and models so that other States/locales seeking to implement effective open adoption programs for youth and sibling groups have a demonstrated resource for