Web at *http://www.whitehouse.gov/infocus/hurricane/*.

This Request for Information is a first step in understanding the availability or feasibility of such services and how the Federal government might encourage citizens to voluntarily maintain critical information so that it can be accessed easily during an emergency. This Request for Information is not intended as a prelude to any procurement by the Federal government. Rather, it is intended to elicit suggestions from members of the public about capabilities that should be considered for maintaining personal information and to provide ideas for consideration as to how to encourage individuals and the private sector to take action in preparation for emergencies.

In particular, HHS seeks to understand the roles and responsibilities of individuals who provide and maintain this information, including the relationship between custodians and individuals who use their services. Respondents should differentiate between capabilities that already exist and those which are planned or desirable in the future.

A separate Request for Information will be published in the **Federal Register** seeking input about the availability or feasibility of electronic benefits services for disaster victims that would facilitate the provision of Federal, state, local, and non-governmental human assistance programs in an efficient manner.

HHS encourages all potentially interested parties—individuals, consumer groups, associations, governments, non-governmental organizations, and commercial entities—to respond. To facilitate review of the responses, please reference the question number in your response.

Questions for Response

1. Approach, Finance, Sustainability, and Roles

a. What models and options are currently available that provide or support the capability to provide ready access to critical documents during or following an emergency?

b. What models and options should be available, that are currently not available, to provide this service? Describe how this approach or model would work and illustrate with examples where useful.

c. How will such a service be made accessible to those it is intended to help?

d. How would accessibility for persons with special needs (e.g. persons with disabilities, persons who are not proficient in English) be ensured?

e. What ownership, management, governance, financing, and sustainability issues arise as a result of the recommended approach, and how should these issues be resolved?

f. How should the effort(s) be funded? Who should pay for the service and infrastructure?

2. Function, Capabilities, and Performance

a. What types of information do you view as relevant, necessary, or useful to access in an emergency (e.g., birth certificates, wills, medical information)? Of these types of information, which would be easy to deposit with the type of service contemplated in this Request for Information (RFI), which would be difficult, and why?

b. What is the best approach for storage and retrieval of this information?

c. What limits should there be on the availability of information via the service contemplated by this RFI, and how should those limits be implemented?

d. What are the necessary features, capabilities, and attributes of the service contemplated by this RFI?

e. How should this service support disaster survivors in providing documentation necessary to obtain Federal, local, and non-governmental disaster relief benefits?

f. What are the performance requirements of the service or the system that supports it?

g. What disclosures should be required and under what circumstances or conditions would such disclosures be made?

3. Rights, Rules, Responsibilities, and Enforcement

a. Whom do you view as the interested parties? How should interested parties interact? What are their roles and responsibilities?

b. What is an inappropriate disclosure? Who has liability for inappropriate or unlawful disclosures, or harms that come as a result of storage of personal data?

c. What enforcement mechanisms are appropriate to protect information, and who should be responsible for enforcement?

d. What rights should individuals who deposit their information have with respect to the custodian?

e. What rights should be assigned to custodians providing the service?

f. What data disclosure laws and policies should apply? Who will have access to the information, and under what circumstances?

g. What other types of rules should apply to the service?

h. What legal implications are there, if any, of storing electronic copies of important documents and making them available via such a service to those permitted to receive the information? If there are impediments, how should they be overcome? (For example, how will the contents of documents be authenticated?)

i. If residents of one State are permitted to store their documents in another State, how would protections travel across States?

4. Security and Standards

a. What administrative, technical, and physical security approaches should be considered?

b. What security standards mechanisms, if any, should be adopted by or imposed on the custodians?

c. How will access and authentication controls be implemented?

d. What technical, data, format, or performance standards should be considered?

e. How will the identity of the individual requesting information be verified?

5. Potential Federal Roles

a. What role, if any, should the Federal government play in encouraging the development of services whereby individuals can voluntarily deposit their personal identifying information for access during or following an emergency?

b. What role, if any, should the Federal government play in encouraging citizens to voluntarily collect and store their personal information for access during or following an emergency?

Please feel free to add any other comments, suggestions, or creative ideas to your response.

Issued on May 17, 2006.

Charles Havekost,

Deputy Assistant Secretary for Information Technology and Chief Information Officer.

[FR Doc. E6–7833 Filed 5–22–06; 8:45 am]

BILLING CODE 4150–37–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Centers for Medicare & Medicaid Services

Privacy Act of 1974; Report of a Modified or Altered System of Records

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

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

SUMMARY: In accordance with the Privacy Act of 1974, we are proposing to modify or alter an existing SOR, ''Automated Survey Processing Environment (ASPEN) Complaints/ Incidents Tracking System (ACTS),'' System No. 09–70–1519, last published at 68 FR 50795 (August 22, 2003). CMS is reorganizing its databases because of the impact of the Medicare Prescription Drug, Improvement, and Modernization Act of 2003 (MMA) (Public Law (Pub. L.) 108–173) provisions and the large volume of information the Agency collects to administer the Medicare program. We propose to assign a new CMS identification number to this system to simplify the obsolete and confusing numbering system originally designed to identify the Bureau, Office, or Center that maintained the system of records. The new assigned identifying number for this system should read: System No. 09–70–0565.

We propose to delete published routine uses number 5 authorizing disclosures to the agency of a state government, number 8 authorizing disclosure to researchers, and number 12 authorizing disclosure to another agency or instrumentality of any governmental jurisdiction. Disclosures permitted under routine uses number 5 and 12 will be made a part of proposed routine use number 2. The scope of routine use number 2 will be broadened to allow for release of information to ''another Federal and/or state agency, an agency established by state law, or its fiscal agent.'' Routine use number 8 is being deleted because disclosure of ACTS data for research and evaluation purposes will be restricted to the release of aggregate data rather than individual-specific data.

CMS proposes to exempt this system from the notification, access, correction and amendment provisions of the Privacy Act of 1974 (5 U.S.C. 552a (k) (2)) due to investigatory and law enforcement activities.

We are modifying the language in the remaining routine uses to provide a proper explanation as to the need for the routine use and to provide clarity to CMS's intention to disclose individual-specific information contained in this system. The routine uses will then be prioritized and reordered according to their usage. We will also take the opportunity to update any sections of the system that were affected by the recent reorganization or MMA provisions and to update language in the administrative sections to correspond with language used in other CMS SORs. The primary purpose of this modified system is to track and process complaints and incidents reported against Medicare and/or Medicaid certified providers and suppliers, and CLIA-certified laboratories, these include: skilled nursing facilities, nursing facilities, hospitals, home health agencies, end-stage renal disease facilities, hospices, rural health clinics, comprehensive outpatient rehabilitation facilities, outpatient physical therapy services, community mental health centers, ambulatory surgical centers, suppliers of portable X-Ray services, and intermediate care facilities for persons with mental retardation. The information retrieved from this system of records will also be disclosed to: (1) Support regulatory, reimbursement, and policy functions performed within the agency or by a contractor, consultant or grantee; (2) assist another Federal or state agency, an agency established by state law, or its fiscal agent; (3) assist Quality Improvement Organizations; (4) support constituent requests made to a Congressional representative; (5) support litigation involving the agency; (6) assist a national accreditation organization that has been granted deeming authority by CMS; (7) assist a state-mandated Protection and Advocacy System that provides legal representation and other advocacy services to beneficiaries; and (8) combat fraud and abuse in certain Federally-funded 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 modified or altered routine uses, CMS invites comments on all portions of this notice. See ''Effective Dates'' section for comment period.

DATES: *Effective Date:* CMS filed a modified or altered SOR report with the Chair of the House Committee on Government Reform and Oversight, the Chair of the Senate Committee on Homeland Security & Governmental Affairs, and the Administrator, Office of Information and Regulatory Affairs, Office of Management and Budget (OMB) on May 16, 2006. To ensure that all parties have adequate time in which to comment, the new system will become effective 30 days from the publication of the notice, or 40 days from the date it was submitted to OMB and the Congress, whichever is later. We may defer implementation of this system 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 comments 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: Cheryl Hatcher, Division of National Systems, Finance, Systems and Budget Group, Center for Medicaid and State Operations, CMS, Mail Stop S3–13–15, 7500 Security Boulevard, Baltimore, Maryland 21244–1850. She can also be reached by telephone at 410–786–3106, or via e-mail at *Cheryl.Hatcher@cms.hhs.gov.*

SUPPLEMENTARY INFORMATION: ACTS is a Windows-based program designed to track and process complaints and incidents reported against health care facilities regulated by CMS and the state agencies. It is designed to manage all operations associated with complaint/ incident tracking and processing, from initial intake and investigation through the final disposition. ACTS allows CMS to track complaints/incidents, allegations, investigations, disposition and certain information for Clinical Laboratory Improvement Amendments of 1988 (CLIA) laboratories.

ACTS is a national tracking system used by the state agencies and CMS. It permits the collection procedures for complaints to be timely, consistent and complete. ACTS is used for all Medicare and/or Medicaid -certified providers and suppliers, and CLIA-certified laboratories. These include: skilled nursing facilities, nursing facilities, hospitals, home health agencies, end-stage renal disease facilities, hospices, rural health clinics, comprehensive outpatient rehabilitation facilities, outpatient physical therapy services, community mental health centers, ambulatory surgical centers, suppliers of portable X-Ray services, intermediate care facilities for persons with mental retardation, and CLIA-certified laboratories.

ACTS maintains Federal complaint information, as well as state licensure complaint information. State licensure information is both relevant and necessary to meet CMS' purposes. Under section 1864(a) of the Social Security Act, the Secretary uses the help of State health agencies, or other appropriate agencies, when determining whether health care entities meet Federal Medicare standards. Also, section 1902(a)(9)(A) of the Social

Security Act requires that a State use this same agency to set and maintain additional standards for the State Medicaid program. Section 1902(a)(33)(B) requires that the state use the agency utilized for Medicare or, if such agency is not the state agency responsible for licensing health institutions, the state use the agency responsible for such licensing to determine whether institutions meet all applicable Federal health standards for Medicaid participation, subject to validation by the Secretary. The state survey agencies perform both Federal certification and state licensure functions, including the investigation of complaints and entity-reported incidents. For example sections 1819(d) and 1919(d) of the Social Security Act require licensure under applicable state and local laws for skilled nursing and nursing facilities. In order to encourage efficiency in state operations, ACTS permits collection of Federal and state information, so that the states may maintain only one database, instead of multiple systems. CMS does seek to eliminate duplicative processes and unnecessary burden, to the extent possible, so that the states can achieve more effective management of their certification and licensure responsibilities.

ACTS allows users to distinguish between Federal information and information that is collected for State licensure purposes. ACTS supports the entry of both Federal and State licensure information, thus reflecting the actual business practices of state agencies as they track complaints and incidents. In many areas, ACTS allows entry of both types of information while still maintaining discrete records to support separate and different views, reports and statistics.

I. Description of the Modified or Altered System of Records

A. Statutory and Regulatory Basis for SOR

Authority for maintenance of the system is given under §§ 1819, 1864, 1865, 1867, 1891, 1902(a)(9)(A), 1902(a)(33)(B), and 1919 of the Social Security Act, section 353 of the Public Health Service Act (42 United States Code 263a) and 42 Code of Federal Regulations (CFR) Subchapter G.

B. Collection and Maintenance of Data in the System

ACTS contains information related to allegations of complaints and incidents filed against Medicare and/or Medicaid -certified providers and suppliers and CLIA-certified laboratories. ACTS contains identifiable information on individuals who are complainants, residents/patients/clients, contacts/ witnesses, alleged perpetrators, survey team members, laboratory directors and laboratory owners, including the investigation of complaints and entity-reported incidents. The system contains demographic and identifying data, as well as survey and deficiency data. Identifying data includes, but is not limited to: name, title, address, city, state, ZIP code, e-mail address, telephone numbers, fax number, licensure number, social security number, Federal tax identification number, alias names, date of birth, gender, date admitted and/or date discharged.

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 ACTS 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 ACTS. CMS has the following policies and procedures concerning disclosures of information that will be maintained in the system. Disclosure of information from this system 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 track and process complaints and incidents reported against Medicare and/or Medicaid certified providers and suppliers, and CLIA-certified laboratories, these include: skilled nursing facilities, nursing facilities, hospitals, home health agencies, end-stage renal disease facilities, hospices, rural health clinics, comprehensive outpatient rehabilitation facilities, outpatient physical therapy services, community mental health centers, ambulatory surgical centers, suppliers of portable X-Ray services, and intermediate care facilities for persons with mental retardation.

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, consultants, or to a grantee who have been engaged by the agency to assist in the accomplishment of a CMS function relating to the purposes for this system and who need to have access to the records in order to assist CMS.

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

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, consultant or grantee whatever information is necessary for the contractor, consultant or grantee to fulfill its duties. In these

situations, safeguards are provided in the contract prohibiting the contractor, consultant or grantee from using or disclosing the information for any purpose other than that described in the contract and requires the contractor, consultant or grantee to return or destroy all information at the completion of the contract.

2. To another Federal and/or state agency, an agency established by state law, or its fiscal agent to:

a. Contribute to the accuracy of CMS' proper payment of Medicare benefits,

b. 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, and/or

c. assist Federal/state Medicaid programs within the state.

Other Federal or state agencies in their administration of a Federal health program may require ACTS information in order to support evaluations and monitoring of Medicare claims information of beneficiaries, including proper reimbursement for services provided. ACTS information can also be used to determine overall cost, effectiveness, and the quality of health care and services provided by a Federally-funded health benefits program.

Information from ACTS may also be given to state's Adult Protective Services for the investigation of suspected abuse, neglect, and/or exploitation of adults.

Information from ACTS may also be shared with the state's Long-Term Care Ombudsman program. Under the Older Americans Act, the Long-Term Care Ombudsman addresses complaints and advocated for improvements in the long-term care system.

3. To Quality Improvement Organizations (QIO) in order to assist the QIO to perform Title XI and Title XVIII functions relating to assessing and improving quality of care.

The QIO will work to implement quality improvement programs, provide consultation to CMS, its contractors, and to state agencies. The QIO will assist state agencies in related monitoring and enforcement efforts, assist CMS and intermediaries in program integrity assessment, and prepare summary information for release to CMS.

4. 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 to CMS, and CMS must be able to give sufficient information to be responsive to the inquiry.

5. 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.

6. To a national accreditation organization that has been granted deeming authority or certified by the Secretary for the purpose of improving the quality of care provided through the provision of health care accreditation and related services that support performance improvement and monitors the quality of deemed providers/suppliers through the investigation of complaints. CMS will provide facility information to approved accreditation organizations on their accredited entities that are deemed for participation in the Medicare program.

CMS anticipates that accreditation organizations will have legitimate requests to use these data to investigate complaints and to improve the care provided to patients/clients and the policies that govern the care provided.

7. To a state-designated Protection and Advocacy System that provides legal representation and other advocacy services for the purposes of monitoring, investigating and attempting to remedy adverse conditions, and for responding to allegations of abuse, neglect and violations of the rights of persons with disabilities.

Data will be released to the state-designated Protection and Advocacy System only on those individuals who are identified as patients within the state, or are legal residents of the State, regardless of the location of the facility in which the patient is receiving services.

8. To a CMS contractor (including, but not necessarily limited to Medicare administrative contractors, 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.

9. 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 ACTS information for the purpose of combating fraud and abuse in such Federally-funded programs.

B. Additional Provisions Affecting Routine Use Disclosures

To the extent 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, subparts A and E) 65 FR 82462

(12–28–00). Disclosures of such PHI that are otherwise 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.'' (See 45 CFR 164.512(a)(1)).

In addition, our policy will be to prohibit release even of data not directly identifiable, 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 may apply 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 National Institute of Standards and Technology publications; the HHS Information Systems Program Handbook and the CMS Information Security Handbook.

V. Effects of the Modified or Altered System of Records on Individual Rights

CMS proposes to modify 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 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.

Dated: May 15, 2006.

Charlene Frizzera,

Acting Chief Operating Officer, Centers for Medicare & Medicaid Services.

SYSTEM NO. 09–70–0565.

SYSTEM NAME:

''Automated Survey Processing Environment (ASPEN) Complaints/Incidents Tracking System (ACTS),'' HHS/CMS/CMSO.

SECURITY CLASSIFICATION:

Level Three Privacy Act Sensitive Data.

SYSTEM LOCATION:

The Centers for Medicare & Medicaid Services (CMS) Data Center, 7500 Security Boulevard, North Building, First Floor, Baltimore, Maryland 21244–1850 and at various contractor sites and at CMS Regional Offices.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

ACTS contains information related to allegations of complaints and incidents filed against Medicare/Medicaid-certified providers and suppliers and CLIA-certified laboratories. ACTS contains identifiable information on individuals who are complainants, residents/patients/clients, contacts/witnesses, alleged perpetrators, survey team members, laboratory directors and laboratory owners, including the investigation of complaints and entity-reported incidents.

CATEGORIES OF RECORDS IN THE SYSTEM:

The system contains demographic and identifying data, as well as survey and deficiency data. Identifying data includes, but is not limited to: name, title, address, city, state, ZIP code, e-mail address, telephone numbers, fax number, licensure number, social security number, Federal tax identification number, alias names, date of birth, gender, date admitted and/or date discharged.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Authority for maintenance of the system is given under §§ 1819, 1864, 1865, 1867, 1891, 1902(a)(9)(A), 1902(a)(33)(B), and 1919 of the Social Security Act, section 353 of the Public Health Service Act (42 United States Code 263a) and 42 Code of Federal Regulations (CFR) Subchapter G.

PURPOSE(S) OF THE SYSTEM:

The primary purpose of this modified system is to track and process complaints and incidents reported against Medicare and/or Medicaid certified providers and suppliers, and CLIA-certified laboratories, these include: skilled nursing facilities, nursing facilities, hospitals, home health agencies, end-stage renal disease facilities, hospices, rural health clinics, comprehensive outpatient rehabilitation facilities, outpatient physical therapy services, community mental health centers, ambulatory surgical centers, suppliers of portable X-ray services, and intermediate care facilities for persons with mental retardation. The information retrieved from this system of records will also be disclosed to: (1) Support regulatory, reimbursement, and policy functions performed within the agency or by a contractor, consultant or grantee; (2) assist another Federal or state agency, an agency established by state law, or its fiscal agent; (3) assist Quality Improvement Organizations; (4) support constituent requests made to a Congressional representative; (5) support litigation involving the agency; (6) assist a national accreditation organization that has been granted deeming authority by CMS; (7) assist a state-mandated Protection and Advocacy System that provides legal representation and other advocacy services to beneficiaries; and (8) combat fraud and abuse in certain Federally-funded health benefits programs.

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

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, consultants, or to a grantee who have been engaged by the agency to assist in the accomplishment of a CMS function relating to the purposes for this system and who need to have access to the records in order to assist CMS.

2. To another Federal and/or state agency, an agency established by state law, or its fiscal agent to:

a. Contribute to the accuracy of CMS' proper payment of Medicare benefits,

b. 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, and/or

c. assist Federal/state Medicaid programs within the state.

3. To Quality Improvement Organizations (QIO) in order to assist the QIO to perform Title XI and Title XVIII functions relating to assessing and improving quality of care.

4. 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.

5. 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.

6. To a national accreditation organization that has been granted deeming authority or certified by the Secretary for the purpose of improving the quality of care provided through the provision of health care accreditation and related services that support performance improvement and monitors the quality of deemed providers/suppliers through the investigation of complaints. CMS will provide facility information to approved accreditation organizations on their accredited entities that are deemed for participation in the Medicare program.

7. To a state-designated Protection and Advocacy System that provides legal representation and other advocacy services for the purposes of monitoring, investigating and attempting to remedy adverse conditions, and for responding to allegations of abuse, neglect and violations of the rights of persons with disabilities.

8. To a CMS contractor (including, but not necessarily limited to Medicare administrative contractors, 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.

9. 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: To the extent 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, subparts A and E) 65 FR 82462 (12–28–00). Disclosures of such PHI that are otherwise 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.'' (See 45 CFR 164.512(a)(1)).

In addition, our policy will be to prohibit release even of data not directly identifiable, 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).

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

STORAGE:

All records are stored on the magnetic disk sub-system of the Windows 2000 server. Furthermore, these records are saved to magnetic tape backup on a nightly basis.

RETRIEVABILITY:

The Medicare, Medicaid, and CLIA records are retrieved by name of provider/supplier, Medicare provider number, ACTS Intake ID, state assigned Medicaid number, or other CMS assigned numbers, complainant's name, resident/patient/client's name, contact/witness name, alleged perpetrator's name, survey team member's name, surveyor identification number, laboratory director's name, laboratory owner's name or Federal tax identification number.

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 may apply 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 National Institute of Standards and Technology publications; the HHS Information Systems Program Handbook; and the CMS Information Security Handbook.

RETENTION AND DISPOSAL:

CMS will retain identifiable ACTS data for a total period not to exceed 15 years. All claims-related records are encompassed by the document preservation order and will be retained until notification is received from DOJ.

SYSTEM MANAGER(S) AND ADDRESS:

Director, Division of National Systems, Finance, Systems and Budget Group, Center for Medicaid and State Operations, CMS, Mail Stop S3–13–15, 7500 Security Boulevard, Baltimore, Maryland 21244–1850.

NOTIFICATION PROCEDURE:

For purpose of access, the subject individual should write to the system manager who will require the system name, HICN, provider/supplier's name, date the complaint/incident occurred, address, date of birth, and gender, and for verification purposes, the subject individual's name (woman's maiden name, if applicable), and SSN. Furnishing the SSN is voluntary, but it may make searching for a record easier and prevent delay.

RECORD ACCESS PROCEDURE:

For purpose of access, use the same procedures outlined in Notification Procedures above. Requestors should also specify the record contents being sought. (These procedures are in accordance with department regulation 45 CFR 5b.5(a)(2)).

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:

The following forms and the ACTS software are used to collect ACTS data: Medicare/Medicaid/CLIA Complaint Form (CMS–562); Statement of Deficiencies and Plan of Correction (CMS–2567); Post-Certification Revisit Report (CMS–2567B); Survey Team Composition and Workload Report (CMS–670); Request for Validation of Accreditation Survey for Hospital (CMS–2802); Request for Validation of Accreditation Survey for Laboratory (CMS–2802A); Request for Validation of Accreditation Survey for Hospice (CMS–2802B); Request for Validation of Accreditation Survey for Home Health Agency (CMS–2802C); and Request for Validation of Accreditation Survey for Ambulatory Surgical Center (CMS–2802D). Request for Survey of 489.20 and 489.24 Essentials of Provider Agreements: Responsibilities of Medicare Participating Hospitals in Emergency Cases (CMS–1541A) and CMS–116–CLIA Laboratory Application.

SYSTEMS EXEMPTED FROM CERTAIN PROVISIONS OF THE ACT:

HHS claims exemption of certain records in the system from notification and access procedures under 5 U.S.C. 522a(k)(2) inasmuch as these records are investigatory materials compiled for program (law) enforcement in anticipation of criminal or administrative proceedings. (See Department Regulation (45 CFR 5b.11)).

[FR Doc. E6–7806 Filed 5–22–06; 8:45 am]

BILLING CODE 4120–03–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Administration for Children and Families

Statement of Organization, Functions, and Delegations of Authority

This notice amends Part K of the Statement of Organization, Functions, and Delegations of Authority of the Department of Health and Human Services (DHHS), Administration for Children and Families (ACF), as follows: Chapter KA, Immediate Office of the Assistant Secretary, as last amended at 63 FR 81–87, January 2, 1998; Chapter KB, Administration on Children, Youth and Families (ACYF), as last amended at 67 FR 8816–18, February 26, 2002; and Chapter KH, Office of Family Assistance (OFA), as last amended at 67 FR 67198, November 4, 2002. This reorganization will transfer the Head Start Bureau (KBC) in its entirety and with its current organizational structure, from ACYF (KB), and retitle it as the Office of Head Start (KU) reporting directly to the Assistant Secretary for Children and Families. This reorganization will also transfer the Child Care Bureau (KBG) in its entirety and with its current organizational structure from ACYF to the Office of Family Assistance (KH). The changes are as follows:

I. Under Chapter KB, Administration on Children, Youth and Families, make the following changes:

A. Delete, KB.00 Mission, in its entirety and replace with the following:

KB.00 Mission: The Administration on Children, Youth and Families (ACYF) advises the Secretary, through the Assistant Secretary for Children and Families, on matters relating to the sound development of children, youth and families by planning, developing and implementing a broad range of activities. It administers state grant programs under titles IV–B and IV–E of the Social Security Act; manages the Adoption Opportunities program and other discretionary programs for the development and provision of child welfare services; and administers discretionary grant programs providing facilities for runaway youth; and administers the Child Abuse Prevention and Treatment Act. It supports and encourages services that prevent or remedy the effects of abuse and/or neglect of children and youth.

In concert with other components of ACF, ACYF develops and implements research, demonstration and evaluation strategies for the discretionary funding of activities designed to improve and enrich the lives of children and youth and to strengthen families. It administers Child Welfare Services training and Child Welfare Services research and demonstration programs authorized by title IV–B of the Social Security Act; administers the Runaway and Homeless Youth Act authorized by title III of the Juvenile Justice and Delinquency Prevention Act; and manages initiatives to involve the private and voluntary sectors in the areas of children, youth and families.

B. Under Chapter KB, Paragraph KB.10 Organization, delete the following components in their entireties:

—Head Start Bureau (KBC).
—Child Care Bureau (KBG).

C. Under Paragraph KB.20 Functions, delete Paragraph ''C. Head Start Bureau (KBC),'' and Paragraph ''G. Child Care Bureau (KBG),'' in their entireties, and remove any reporting references to ACYF.

II. Under Chapter KH, Office of Family Assistance, make the following changes:

A. Delete Paragraph, KH.00 Mission in its entirety and replace with the following:

KH.00 Mission: The Office of Family Assistance (OFA) advises the Secretary, through the Assistant Secretary for Children and Families, on matters relating to the Temporary Assistance for Needy Families (TANF) program, title IV–A of the Social Security Act. This program promotes temporary assistance