Medicare & Medicaid Services not later than December 31 of each year.

The Council consists of 15 physicians, each of whom has submitted at least 250 claims for physicians' services under Medicare in the previous year. Members of the Council include both participating and nonparticipating physicians, and physicians practicing in rural and underserved urban areas. At least 11 members of the Council must be physicians described in section 1861(r)(1) of the Act; that is, State-licensed doctors of medicine or osteopathy. The remaining 4 members may include dentists, podiatrists, optometrists, and chiropractors. Members serve for overlapping 4-year terms; terms of more than 2 years are contingent upon the renewal of the Council by appropriate action before its termination. Section 1868(a) of the Act provides that nominations to the Secretary for Council membership must be made by medical organizations representing physicians.

The Council held its first meeting on May 11, 1992. The current members are: James Bergeron, M.D.; Ronald Castallanos, M.D.; Rebecca Gaughan, M.D.; Carlos R. Hamilton, M.D.; Joseph Heyman, M.D.; Dennis K. Iglar, M.D.; Christopher Leggett, M.D.; Joe Johnson, D.O.; Barbara McAneny, M.D.; Angelyn L. Moultrie-Lizana, D.O.; Laura B. Powers, M.D.; Michael T. Rapp, M.D.; Amilu Rothhammer, M.D.; Robert L. Urata, M.D.; and Douglas L. Wood, M.D. Council members will be updated on the status of recommendations made during the past year.

The agenda will provide for discussion and comment on the following topics:

- Physician's Regulatory Issues Team (PRIT) update.
- Physicians Group Practice Demonstrations and proposals for future demonstrations.
- Lowering Medicare Costs: Regions or Beneficiaries?
- Provider Enrollment.
- Authority for Policies on Coverage Procedures and Devices Results in Inequities.
- Practice Patterns for Physicians.
- Doctors' Office Quality Update.
- Overview Prescription Drug Benefit.
- Health Insurance Portability and Accountability Act.
- Limited English Proficiency Requirement.
- Revisions to the Average Wholesale Price Methodology Regulation.

For additional information and clarification on the topics listed, call the contact person in the **FOR FURTHER INFORMATION CONTACT** section of this notice.

Individual physicians or medical organizations that represent physicians wishing to make 5-minute oral presentations on agenda issues should contact one of the Designated Federal Officials by 12 noon, Friday, September 5, 2003, to be scheduled. Testimony is limited to agenda topics. The number of oral presentations may be limited by the time available. A written copy of the presenter's oral remarks should be submitted to Diana Motsiopoulos at *dmotsiopoulos@cms.hhs.gov* no later than 12 noon, September 5, 2003, for distribution to Council members for review before the meeting. Physicians and organizations not scheduled to speak may also submit written comments to the Executive Director and Council members. The meeting is open to the public, but attendance is limited to the space available. Individuals requiring sign language interpretation for the hearing impaired or other special accommodation should contact Diana Motsiopoulos at *dmotsiopoulos@cms.hhs.gov* or (410) 786–3379 at least 10 days before the meeting.

This notice also serves as an invitation to all organizations representing physicians to submit nominees for membership on the Council. Each nomination must state that the nominee has expressed a willingness to serve as a Council member and must be accompanied by a short resume or description of the nominee's experience. To permit an evaluation of possible sources of conflicts of interest, potential candidates will be asked to provide detailed information concerning financial holdings, consultant positions, research grants, and contracts. Section 1868(b) of the Act provides that the Council meet quarterly to discuss certain proposed changes in regulations and manual issuances that relate to physicians' services, identified by the Secretary. Council members are expected to participate in all meetings. Section 1868(c) of the Act provides for payment of expenses and a per diem allowance for Council members at a rate equal to payment provided members of other advisory committees. In addition to making these payments, the Department of Health and Human Services/Centers for Medicare & Medicaid Services provides management and support services to the Council. The Secretary will appoint new members to the Council from among those candidates determined to have the expertise required to meet specific agency needs and in a manner to ensure appropriate balance of the Council's membership.

Authority: (Sec. 1868 of the Social Security Act (42 U.S.C. 1395ee) and sec. 10(a) of Pub. L. 92–463 (5 U.S.C. App. 2, sects. 10(a) and 14).

(Catalog of Federal Domestic Assistance Program No. 93.773, Medicare—Hospital Insurance; and Program No. 93.774, Medicare—Supplementary Medical Insurance Program)

Dated: August 7, 2003.

Thomas A. Scully,

Administrator, Centers for Medicare & Medicaid Services.

[FR Doc. 03–21442 Filed 8–21–03; 8:45 am]

BILLING CODE 4120–01–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Centers for Medicare and Medicaid Services

Privacy Act of 1974; Report of New System

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

ACTION: Notice of new system of records.

SUMMARY: In accordance with the requirements of the Privacy Act of 1974, we are proposing to establish a new system of records. The proposed system is titled, ''ASPEN Complaints/Incidents Tracking System (ACTS), HHS/CMS/CMSO, 09–70–1519.'' The primary purpose of the system of records is to track and process complaints and incidents reported against Medicare/Medicaid/CLIA providers and suppliers, and to maintain information on laboratory directors and owners. ACTS is a windows-based, program designed to track and process complaints and incidents reported against health care facilities regulated by the Centers for Medicare and Medicaid Services (CMS). 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 CLIA laboratories.

Information retrieved from this system of records will also be used to aid in the administration of the survey and certification of Medicare/Medicaid/CLIA providers and suppliers; support agencies of the State governments to determine, evaluate and assess overall effectiveness and quality of provider/supplier services provided in the State; aid in the administration of Federal and

State programs within the State; support constituent requests made to a Congressional representative, support litigation involving the agency, and facilitate research on the quality and effectiveness of care provided. We have provided background information about the proposed system in the **SUPPLEMENTARY INFORMATION** section below. Although the Privacy Act requires only that the ''routine use'' portion of the system be published for comment, CMS invites comments on all portions of this notice. See **EFFECTIVE DATES** section for comment period.

EFFECTIVE DATES: CMS filed a new system 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 August 8, 2003.

ADDRESSES: The public should address comments to: Director, Division of Privacy Compliance Data Development (DPCDD), CMS, Room 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 time zone.

FOR FURTHER INFORMATION CONTACT: Wayne Smith, Finance, Systems and Budget Group, Center for Medicaid and State Operations, Centers for Medicare and Medicaid Services, 7500 Security Boulevard, Room S3–18–11, Baltimore, Maryland 21244–1850, Telephone Number: (410) 786–3258.

Steven Pelovitz, Survey and Certification Group, Center for Medicaid and State Operations, Centers for Medicare and Medicaid Services, 7500 Security Boulevard, Room S2–12–25, Baltimore, Maryland 21244–1850, Telephone Number: (410) 786–3160.

SUPPLEMENTARY INFORMATION:

I. Description of the Proposed System of Records

A. Glossary of Terms

ACTS—ASPEN Complaints/Incidents Tracking System.

ASPEN—Automated Survey Processing Environment.

CLIA—Clinical Laboratory Improvement Amendments of 1988.

OSCAR—Online Survey Certification and Reporting System.

B. Background

The implementation of ACTS is critical to CMS's mission of assuring that beneficiaries receive quality care in a safe environment. Several reports in recent years have highlighted this need. In March 1999, the General Accounting Office (GAO) issued a report entitled, ''Complaint Investigation Processes Often Inadequate to Protect Residents.'' GAO assessed the effectiveness of State complaint investigation practices and the role of CMS in establishing standards and conducting oversight. The GAO recommended stronger requirements, increased federal monitoring and improved tracking of findings for complaints. In addition, in 1999, the Office of the Inspector General (OIG) issued a report entitled ''The External Review of Hospital Quality.'' OIG recommended that CMS hold accreditation agencies and State agencies more fully accountable for their performance in reviewing hospitals. One of the areas that OIG made specific recommendations about was the handling of complaints. ACTS is part of CMS'' response to these recommendations.

The ACTS responds to the concerns and problems found by the GAO, OIG and CMS'' own needs. The ability to capture data that are useful, analyze data in a meaningful way, and use the products of the analysis to make refinements and improvements is critical to continuous quality improvement. Before ACTS, complaint data was maintained in the OSCAR Complaint System. The OSCAR Complaint System collected a minimal amount of data that was the result of an onsite survey. The data in ACTS is much more comprehensive than data that was maintained in the OSCAR Complaint System. ACTS automates complaint management operations. ACTS is a windows-based, client-server application that tracks, processes, and reports on complaints/incidents made against certified health care providers and suppliers. It is designed to manage all operations associated with complaints/incidents processing, from initial intake and investigation through final disposition. It is fully integrated into the ASPEN standard system architecture. Specific fields are configurable by individual states to accommodate a variety of operations environments.

ACTS is a national tracking system used by all States. It permits the collection procedures for complaints to be timely, consistent and complete. ACTS will eliminate redundant data collection systems, and it takes advantage of new technology and open systems architecture. ACTS will be used for all certified providers and suppliers. These providers and suppliers 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, federally qualified health centers, ambulatory surgical centers, portable X-Ray facilities, intermediate care facilities for persons with mental retardation, and CLIA laboratories. Data in ACTS is collected and entered by the State Survey Agencies and CMS Regional Offices.

C. Statutory and Regulatory Basis for System of Records

Section 1864 of the Social Security Act (the Act) states the Secretary may use State agencies to determine compliance by providers of services with the conditions of participation. Under section 1864(a) the 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 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. Sections 1819(d) and 1919(d) of the Act require licensure under applicable State and local laws.

Sections 1864 (c) and 1865 of the Act provides the basis for conducting complaint surveys of accredited hospitals and establishes the basic framework of complaint surveys for virtually all other accredited providers and suppliers. Regulations authorizing such surveys are found in 42 CFR 488.7(a)(2). 42 CFR 488.332 authorizes investigation of complaints of violations and monitoring of compliance. 42 CFR 488.335 authorizes actions on complaints of resident neglect and abuse, and misappropriation of resident property for nursing homes. 42 CFR 482.13(f) requires a hospital to report any death that occurs while a patient is restrained or in seclusion for behavior management, or where it is reasonable to assume that a patient's death is a

result of restraint or seclusion. 42 CFR 483.13 also requires nursing homes to ensure that all alleged violations involving mistreatment, neglect, abuse, including injuries of unknown source, and misappropriation of resident property are reported immediately to the administrator of the facility and to other officials in accordance with State law through established procedures, including to the State survey and certification agency. Section 353 of the Public Health Service Act (42 U.S.C. 263a) authorizes collection of information from any person or entity seeking certification under CLIA.

The Privacy Act of 1974 requires Federal agencies to implement and publish procedures for the collection, maintenance, and storage of personal information. It requires that the information be gathered only for lawful purposes and that the disclosure of personally identifiable records must be limited and safeguarded. The Privacy Act allows disclosure of an individual's data without consent, given that the data will be used for a purpose that is compatible with the purpose for which the information was collected.

II. Collection and Maintenance of Data in the System

A. Scope of the Data Collected

ACTS tracks allegations of complaints made against providers and suppliers. ACTS includes demographic data for identification of providers/suppliers, such as the Medicare identification number, name of the facility, address, city, state and ZIP code. ACTS contains data for identification of complainants, residents/patients, contacts/witnesses, alleged perpetrators, survey team members, laboratory directors, and laboratory owners. Complainant information includes: Name, title, address, city, state, ZIP code, telephone numbers, e-mail address, and relationship to beneficiary, if applicable. Contacts/Witnesses information includes: Name, title, address, city, state, ZIP code, telephone numbers, fax, and a field to indicate if the individual is a possible witness. Resident/patient information includes: Name, title, date of birth, gender, date admitted, date discharged, location, and room. ACTS also contains information related to any resident/patient deaths that are associated with the use of restraints or seclusion. This information includes: Name, death type (restraint or seclusion) and date of death. Alleged Perpetrator information includes: Name, title, address, city, state, ZIP code, telephone numbers, license number, social security number and Alias name, if any. Survey Team information includes: Name, title, and surveyor identification number. Contact/Witnesses, Resident/Patient and Alleged Perpetrator are not mandatory fields in the ACTS database. These are optional data fields. ACTS will also maintain information for CLIA laboratories. Identifiable information for CLIA laboratories includes: Laboratory director's name, laboratory owner's name and Federal Tax Identification Number.

ACTS will maintain 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 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 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. In fact, sections 1819(d) and 1919(d) of the Act require licensure under applicable State and local laws. 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.

There are mechanisms in ACTS that allow users to distinguish between information that is collected for the purpose of meeting the 1864 Agreement from 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. Federal and State licensure data are stored in the same tables in the database. However, Federal and State licensure data is easily discernable and separate. For reporting purposes, ACTS allows users to exclude complaint and incidents against state licensure only facilities using Facility Type filters. Report customization features in ACTS also allow users to include or exclude complaints or incidents that contain only State-licensure elements.

B. 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, which is compatible with the purpose(s) for which the information was collected. Any such disclosure of data is known as a ''routine use.'' CMS has the following policies, procedures and restrictions on routine use disclosures of information that will be maintained in the system. In general, disclosure of information from the system of records will be approved only for the minimum information necessary to accomplish the purpose of the disclosure after CMS:

(a) Determines that the use or disclosure is consistent with the reason that the data is being collected, *e.g.*, track and process complaints and incidents reported against Medicare/Medicaid/CLIA providers and suppliers, and to maintain information on laboratory directors and owners.

(b) Determines:

(1) That the purpose for which the disclosure is to be made can only be accomplished if the record is provided in individually identifiable form;

(2) That 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

(3) That there is a strong probability that the proposed use of the data would in fact accomplish the stated purpose(s).

(c) Requires the information recipient to:

(1) Establish administrative, technical, and physical safeguards to prevent unauthorized use of disclosure of the record;

(2) Remove or destroy at the earliest time all patient-identifiable information; and

(3) Agree not to use or disclose the information for any purpose other than the stated purpose under which the information was disclosed.

(d) Determines that the data are valid and reliable.

(e) Secure a written statement or agreement from the prospective recipient if the information whereby the prospective recipient attests to an understanding of, and willingness to abide by, the foregoing provisions and any additional provisions that CMS deems appropriate in the particular circumstance.

III. Proposed Routine Use Disclosures of Data in the System

A. Entities Who May Receive Disclosure Under Routine Use

The routine use disclosures of identifiable data for ACTS may occur to the following categories of entities. In addition, our policy will be to prohibit release even of non-identifiable data beyond the listed categories, if there is a possibility that an individual can be identified through implicit deduction based on small cell sizes.

1. 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 whether 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 the use of such records by the DOJ, court or adjudicatory body is therefore deemed by the agency to be for a purpose that 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. A determination would be made in each instance that, under the circumstances involved, the purposes served by the use of the information in the particular litigation is compatible with a purpose for which CMS collects the information.

2. 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. Recipients shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 52a(m).

We contemplate disclosing information under this routine use only in situations in which CMS may enter into a contract or similar agreement with a third party to assist in accomplishing CMS functions relating to purposes for this system of 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 whatever information is necessary for the contractor to fulfill its duties. In these situations, safeguards are provided in the contract prohibiting the contractor from using or disclosing the information for any purpose other than that described in the contract and requires the contractor to return or destroy all information at the completion of the contract.

3. To a CMS contractor (including, but not 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 contract or similar agreement with a third party to assist in accomplishing CMS functions relating to purposes for this system of records.

4. To a Quality Improvement Organization (QIO) in order to assist the QIO to perform Title XI and Title XVIII functions relating to assessing and improving quality of care. QIO's work to implement quality improvement programs; provide consultation to CMS, its contractors, and to State agencies. The QIO's provide a supportive role to health care facilities in their endeavors to comply with Medicare Conditions of Participation; assist State agencies in related monitoring and enforcement efforts; assist CMS in program integrity assessment; and prepare summary information about the nation's health care for release to beneficiaries.

5. To the agency of a State Government, or established by State law, for purposes of determining, evaluating and/or assessing overall or aggregate cost, effectiveness, and/or the quality of services provided in the State; for developing and operating Medicaid reimbursement systems; or for the purpose of administration of Federal/State program within the State. Data will be released to the State only on those individuals who are either 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.

6. To a Federal or State agency (*e.g.*, State Medicaid agencies) to contribute to the accuracy of CMS's health insurance operations (payment, treatment and coverage) and/or to support State agencies in the evaluation and monitoring of care. Data may be released to State agencies such as State Ombudsmen, State Licensing Boards, and Adult Protective Services.

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. Releases of information would be allowed if the proposed use(s) for the information proved compatible with the purpose for which CMS collects the information.

7. To another Federal agency (*e.g.*, Office of the Inspector General, General Accounting Office) 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 (*e.g.*, Medicaid Fraud Control Units) may require ACTS information for combating fraud and abuse in such federally funded programs. Releases of information would be allowed if the proposed use(s) for the information proved compatible with the purposes of collecting the information.

8. To an individual or organization for research, evaluation, or epidemiological project related to the prevention of disease or disability, or the restoration or maintenance of health, and for payment related projects.

CMS anticipates that many researchers will have legitimate requests to use these data in projects that could ultimately improve the care provided to Medicare and Medicaid patients and the policy that governs the care. CMS understands the concerns about the privacy and confidentiality of the release of data for a research use. Disclosure of ACTS data for research and evaluation purposes will usually involve aggregate data rather than individual-specific data.

9. 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, as well as other individuals, may 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.

10. To a national accreditation organization that has been granted deeming authority by CMS 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 (*e.g.*, JCAHO, AOA, AAAASF, AAAHC, AABB, ASHI, CAP, CARF, CHAP, COLA).

11. To a Protection and Advocacy Group 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.

12. To another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States (including any State or local law enforcement agencies) for a civil or criminal law enforcement activity (*e.g.*, police, FBI, State Attorney General's office).

B. Additional Provisions Affecting Routine Use Disclosures

In addition, CMS policy will be to prohibit release even of non-identifiable data, except pursuant to one of the routine uses, if 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).

This System of Records contains Protected Health Information as defined by the Department of Health and Human Services' 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.''

IV. Safeguards

The ACTS system conforms to applicable laws and policy governing the privacy and security of Federal automated information systems. These include but are not limited to: the Privacy Act of 1974, 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''. CMS has prepared a comprehensive System Security Plan as required by OMB Circular A–130, Appendix III. This plan conforms 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.'' Paragraphs A–C of this section highlight some of the specific methods that CMS is using to ensure the security of this system and the information within it.

A. Authorized Users and Access Control

Personnel having access to the system have been trained in Privacy Act and system security requirements. Employees and contractors who maintain records in the system are instructed not to release any data until the intended recipient agrees to implement appropriate administrative, technical, procedural, and physical safeguards sufficient to protect the confidentiality of the data and to prevent unauthorized access to the data. In addition, CMS monitors authorized users to ensure against excessive or unauthorized use. Records are used in a designated work area and system location is attended at all times during working hours.

To ensure security of the data, authentication and access control profiles are maintained within both the database and the ACTS application system used to view information in the database. Within the database access, control is implemented by assigning the proper access profile for each individual user as determined at the State agency level. This prevents unauthorized users from accessing and modifying critical data using other system tools not provided by CMS.

Database-level Protections: The State database upon which ACTS operates includes five classes of database users:

- Database Administrator class owns the database objects; *e.g.*, tables, triggers, indexes, stored procedures, packages and has database administration privileges to these objects;
- Quality Control Administrator class has read and write access to key fields in the database;
- ASPEN User class provides read and write access to tables and fields, which are required to support complaint, survey and related activities.
- Quality Indicator Report Generator class has read-only access to all fields and tables;
- Policy Research class has query access to tables, but are not allowed to access confidential patient identification information.

ACTS Application-Level Protections: All ASPEN applications, including ACTS, provide user login/password authentication, which is tied directly to each State's internal network user login process. Internal application access controls, which secure system functions to pre-approved user groups, are also a key safeguard controlling user access to functions and data. ACTS application and related database safeguards include:

- *Application login:* All ASPEN users must be authenticated to their State or CMS regional office network as a pre-requisite for starting an ASPEN application. This is enforced internally by the ASPEN application. Thus, only known, pre-authenticated users may start an ASPEN application.
- *Application access control:* Once authenticated, ASPEN users may only view information and perform tasks according to pre-assigned security and access control profiles determined by the system administrator. Security profiles may be assigned down to the level of individual menu functions, action buttons and form displays. This means ASPEN allows State and CMS RO administrators to finely tune which users may view certain information and perform specific tasks within the system (such as adding or modifying complaint information). Thus, while a complaint investigator may be able to update findings for a specific complaint, they may be prohibited through their security profile from removing complaints from the system.
- *Provider Type Access Control:* In addition to the data and access control security just described, ASPEN allows administrators to specify user access to information based on provider category. For example, while an investigator may have a security profile that enables the investigator to add findings to a complaint, the system administrator may limit this user to specific categories of providers/suppliers, such as nursing homes—thus, preventing the user from changing findings of complaints for other types of providers/suppliers. An

ASPEN user must have both a security profile that allows a specific function to be performed, and be assigned to appropriate Provider Type access before a specific system action may be taken against a provider/supplier type.

• *Secondary Database Access Control:* Since ASPEN provides an Application-centric security model, it is not necessary to assign each ASPEN user an individual Oracle user name, password and Oracle profile. Instead, all ASPEN users share a single Oracle login whose password is known only by CMS. This protects against a significant threat to data integrity: access to the Oracle database using non-ASPEN system tools; thus, preventing accidental or malicious bypassing of the ASPEN security controls through third-party system tools which may be capable of connecting to Oracle databases. ACTS users may only access ASPEN data via the security-controlled environment of the ACTS application.

• *Audit trail:* ACTS maintains an audit trail for key information elements in the database. Any changes made to these elements via the ACTS system are logged. The log includes information on which element was changed, who changed it, the time of change and prior and current values for the element.

B. Physical Safeguards

All server sites have implemented the following minimum requirements to assist in reducing the exposure of computer equipment and thus achieve an optimum level of protection and security for the ACTS system:

Access to all servers is controlled, with access limited to only those support personnel with a demonstrated need for access. Servers are to be kept in a locked room accessible only by specified management and system support personnel. Each server requires a specific log-on process. All entrance doors are identified and marked. A log is kept of all personnel who were issued a security card, key and/or combination that grants access to the room housing the server, and all visitors are escorted while in this room. All servers are housed in an area where appropriate environmental security controls are implemented, which include measures implemented to mitigate damage to Automated Information Systems resources caused by fire, electricity, water and inadequate climate controls.

Protection applied to the system administration workstations and the Windows 2000 servers, which house the ACTS Oracle database, include:

• User Log-ons—Authentication is performed by the Windows 2000 Primary Domain Controller/Backup Domain Controller of the log-on domain.

• Workstation Names—Workstation naming conventions may be defined and implemented at the State agency level.

• Hours of Operation—May be restricted by Windows 2000. When activated all applicable processes will automatically shut down at a specific time and not be permitted to resume until the predetermined time. The appropriate hours of operation are determined and implemented at the State agency level.

• Inactivity Log-out—Access to the 2000 workstation is automatically logged out after a specified period of inactivity.

• Warnings—Legal notices and security warnings display on all servers and workstations.

There are several levels of security found in the overall ASPEN system. Windows 2000 servers provide much of the overall system security. The Windows 2000 security model is designed to meet the C2-level criteria as defined by the U.S. Department of Defense's Trusted Computer System Evaluation Criteria document (DoD 5200.28–STD, December 1985). Other non-ACTS CMS functions are supported on the same Windows 2000/Oracle servers as ACTS—such as MDS submission from facilities. Such operations are performed via separate Netscape Enterprise Server, which provides an additional layer of user authentication, security and access control. In this case, Netscape controls all CMS information access requests. Anti-virus system is applied at both the system administration workstation and Windows 2000 server levels.

Access to different areas on the Windows NT server is maintained through the use of file, directory and share level permissions. These different levels of access control provide security that is managed at the user and group level within the Windows 2000 server domain. The file and directory level access controls rely on the presence of a Windows NT File System (NTFS) hard drive partition. This provides the most robust security and is tied directly to the file system. Windows 2000 security is applied at both the workstation and Windows 2000 server levels.

Firewalls have been installed on each State server. Appendix A lists the location of each State server. A firewall is a security feature that does not allow unwanted or unsolicited network traffic to flow to certain parts of the system. A Cisco 3640 router is installed at each state. These routers have been programmed to allow the state IP addresses to access certain locations within the CMS network. CMS contractors set up and manage the routers. Using CMS specifications, they have installed the allowed IP's to the router tables. If an unauthorized IP tries to access the CMS data, the firewall (router) will pass the request away from its intended destination. That is, if the firewall does not match the IP of the request to an allowed IP in its table, the request will not be fulfilled. CMS contractors monitor the firewalls and review them for anomalies that could represent a hacking attempt or a hardware problem.

C. Procedural Safeguards

All automated systems must comply with Federal and State laws, guidance, and policies for information systems security, as stated previously in this section. Each State must ensure a level of security commensurate with the level of sensitivity of the data, risk, and magnitude of the harm that may result from the loss, misuse, disclosure, or modification of the information contained in the system.

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 and the State Survey Agencies will monitor the collection and reporting of ACTS data.

CMS and the State Survey Agencies 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 individuals whose data are maintained in the system. CMS will collect only that information necessary to perform the system's functions.

To ensure data that resides in a CMS Privacy Act System of Records; to ensure the integrity, security, and confidentiality of information maintained by CMS; and to permit appropriate disclosure and use of such data as permitted by law, CMS and the non-CMS recipient of the data, hereafter termed ''User,'' enter into an agreement to comply with the following specific requirements. The agreement addresses the conditions under which CMS will disclose and the user will obtain and use the information contained in the system of records. The parties mutually agree that CMS retains ownership rights to the data and that the user does not

obtain any right, title, or interest in any of the data furnished by CMS. The user represents and warrants further that the facts and statements made in any study or research protocol or project plan submitted to CMS for each purpose are complete and accurate. The user shall not disclose, release, reveal, show, sell, rent, lease, loan, or otherwise grant access to the data disclosed from the system of records to any person. The user agrees that access to the data shall be limited to the minimum number of individuals necessary to achieve the purpose stated in the protocol and to those individuals on a need to know basis only. If CMS determines or has reasonable belief that the user has made an unauthorized disclosure of the data, CMS in its sole discretion may require the user to: (a) Promptly investigate and report to CMS any alleged or actual unauthorized disclosures; (b) promptly resolve any problems identified by the investigation; (c) submit a formal response to any allegation of unauthorized disclosures; (d) submit a corrective action plan with steps to prevent any future unauthorized disclosures; and (e) return data files to CMS. If CMS determines or has reasonable belief that unauthorized disclosures have taken place, CMS may refuse to release further CMS data to the user for a period to be determined by CMS.

The Privacy Act provides criminal penalties for certain violations. The Act provides that ''Any officer or employee of an agency, who by virtue of his (or her) employment or official position, has possession of, or access to agency records which contain individually identifiable information the disclosure of which is prohibited by this section or by rules or regulations established there under, and who knowing that disclosure of the specific materials is so prohibited, willfully discloses the material in any manner to a person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000'' (5 U.S.C. 552a(i)(1)). The Act also provides that ''Any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses shall be guilty of a misdemeanor and fined not more than $5,000'' (5 U.S.C. 552a(i)(3)). The agency's contractor and any contractors' employees who are covered by 5 U.S.C. 552a(m)(1) are considered employees of the agency for the purposes of these criminal penalties.

CMS, therefore, does not anticipate an unfavorable effect on individual privacy as a result of the disclosure of information relating to individuals.

Dated: August 8, 2003.

Thomas A. Scully,

Administrator, Centers for Medicare & Medicaid Services.

System No. 09–70–1519

SYSTEM NAME:

ASPEN Complaints/Incidents Tracking System (ACTS).

SECURITY CLASSIFICATION:

Level Three Privacy Act Sensitive Data.

SYSTEM LOCATION:

CMS Data Center, 7500 Security Boulevard, North Building, First Floor, Baltimore, Maryland 21244–1850. Federal Servers are located at each State agency. Appendix A lists the location of each State server.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Identifiable information will be retained in the system of records for individuals who are complainants, residents/clients, contacts/witnesses, alleged perpetrators, survey team members, laboratory directors, and laboratory owners.

CATEGORIES OF RECORDS IN THE SYSTEM:

ACTS contains information related to allegations of complaints and incidents filed against Medicare, Medicaid or CLIA certified providers or suppliers. The system contains demographic and identifying data, as well as survey and deficiency data. Identifying data includes: Names, 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.

ACTS maintains Federal complaint information, as well as state licensure complaint information. State licensure information is both relevant and necessary to meet CMS'' purposes. CMS uses the help of State health agencies, or other appropriate agencies, when determining whether health care entities meet Federal Medicare standards. The State survey agencies perform both Federal certification and State licensure functions, including the investigation of complaints and entity-reported incidents. The Social Security Act requires that providers/suppliers receive licensure under applicable State and local laws. In order to encourage efficiency in State operations, ACTS permits collection of Federal and State information. 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.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Sections 11819(d), 1864, 1865, 1902(a)(9)(A), 1902(a)(33)(B), and 1919(d) of the Social Security Act. Section 353 of the Public Health Service Act (42 U.S.C. 263a), 42 CFR 482.13(f), 42 CFR 483.13, 42 CFR 488.7(a)(2), 42 CFR 488.332, and 42 CFR 488.335.

PURPOSE(S):

The primary purpose of the system of records is to track and process complaints and incidents reported against Medicare/Medicaid/CLIA providers and suppliers, and to maintain information on laboratory directors and owners.

ACTS provides access to survey and provider/supplier information for data-driven analysis and evaluation. This system will improve CMS's ability to monitor the performance of State Survey Agencies including analyzing program variations and more effectively managing program costs. Information retrieved from this system of records will be used to aid in the administration of the survey and certification of Medicare/Medicaid/CLIA providers and suppliers; support agencies of the State governments to determine, evaluate and assess overall effectiveness and quality of provider/supplier services provided in the State; aid in the administration of Federal and State programs within the State; support constituent requests made to a Congressional representative, support litigation involving the agency, and facilitate research on the quality and effectiveness of care provided.

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. We are proposing to establish the following routine use disclosures of information maintained in the system:

1. 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 when 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 the use of such records by the DOJ, court or adjudicatory body is therefore deemed by the agency to be for a purpose that is compatible with the purpose for which the agency collected the records.

2. 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.

3. To a CMS contractor (including, but not necessarily limited to fiscal intermediaries and carriers) that assists in the administration of a CMS-administrated health benefits program, or to a grantee of a CMS-administered health benefits 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.

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

5. To the agency of a State Government, or established by State law, for purposes of determining, evaluating and/or assessing overall or aggregate cost, effectiveness, and/or the quality of services provided in the State; for developing and operating Medicaid reimbursement systems; or for the purpose of administration of Federal/State programs within the State.

6. To a Federal or State agency (*e.g.*, State Medicaid agencies) to contribute to the accuracy of CMS's health insurance operations (payment, treatment and coverage) and/or to support State agencies in the evaluation and monitoring of care.

7. To another Federal agency (*e.g.*, Office of the Inspection General, General Accounting Office, Medicaid Fraud Control Unit) 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.

8. To an individual or organization for research, evaluation, or epidemiological project related to the prevention of disease or disability, the restoration or maintenance of health, or payment related projects.

9. 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.

10. To a national accreditation organization that has been granted deeming authority by CMS 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.

11. To a Protection and Advocacy Group 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.

12. To another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States (including any State or local law enforcement agencies) for a civil or criminal law enforcement activity (*e.g.*, police, FBI, State Attorney General's office).

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 Complaint number, State assigned Medicaid number, or other CMS assigned numbers, complainant's name, resident/patient's name, contact/witnesses 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 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 systems security requirements. Employees who maintain records in the system are instructed not to release any data until the intended recipient agrees to implement appropriate administrative, technical, procedural, and physical safeguards sufficient to protect the confidentiality of the data and to prevent unauthorized access to the data.

In addition, CMS has physical safeguards in place to reduce the exposure of computer equipment and thus achieve an optimum level of protection and security for the ACTS system. For computerized records, safeguards have been established in accordance with the Department Health and Human Services standards and National Institute of Standards and Technology guidelines, *e.g.*, security codes will be used, limiting access to authorized personnel. System securities are established in accordance with HHS, Information Resource Management Circular #10, Automated Information System Security Program; CMS Automated Information Systems (AIS) Guide, Systems Securities Policies, and OMB Circular No. A–130 (revised), Appendix III.

RETENTION AND DISPOSAL:

CMS will retain identifiable ACTS data for a total period not to exceed 15 years.

SYSTEM MANAGER(S) AND ADDRESS:

Director, Finance, Systems and Budget Group, Center for Medicaid and State Operations, Centers for Medicare & Medicaid Services, 7500 Security Boulevard, Baltimore, Maryland 21244–1850.

Director, Survey and Certification Group, Center for Medicaid and State Operations, Center for Medicaid and State Operations, 7500 Security Boulevard, Baltimore, Maryland 21244–1850.

NOTIFICATION PROCEDURE:

For the purpose of accessing records based on individual identifiable data, the subject individual should write to the system manager who will require the system name, Medicare provider/supplier identification number, provider/supplier's name and address, and for verification purposes the subject

individual's name, social security number (SSN) (furnishing the SSN is voluntary, but it may make searching for a record easier and prevent delay), address, date of birth and sex.

RECORD ACCESS PROCEDURE:

For accessing records based on individual identifiable data, use the same procedures outlined in Notification Procedures above. Requestors should also reasonably specify the record contents being sought. (These procedures are in accordance with Department regulation 45 CFR 5b.5(a)(2).)

CONTESTING RECORD PROCEDURES:

The subject individual should contact the system manager named above, and reasonably identify the record 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).

RECORD 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).

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).

CMS–116—CLIA Laboratory Application.

SYSTEMS EXEMPTED FROM CERTAIN PROVISIONS OF THE ACT:

Waiver of 40 day waiting period.

Appendix A Location of State Servers

North Dakota Department of Health Resources, 600 East Boulevard Avenue, Suite 206, Bismarck, ND 58505.

Department of Health, Facility Licensing and Certification Bureau, 2040 South Pacheco, Colgate Building 2nd Floor, Santa Fe, NM 87505.

Utah Department of Health, M/M Program Certification, 288 North, 1460 West, Salt Lake City, UT 84114–2905.

Department of Public Health and Human Services, Senior and Long Term Care Division, 111 Sanders Avenue, Suite 210, P.O. Box 4210, Helena, MT 59601.

Division of Medicaid, Bureau of Facility Standards, Myers & Stauffer, 8555 West Hackamore Dr., Suite 100, Boise, ID 83709–1665.

Rhode Island Department of Health, Three Capitol Hill, Cannon Building, Room 306, Providence, RI 02908–5097.

State of Connecticut, Department of Public Health, 410 Capitol Avenue MS#13DPR, P.O. Box 340308, Hartford, CT 06134–0308.

Minnesota Department of Health, F&PC Division, 85 East 7th Place-Suite 300, P.O. Box 64900, St. Paul, MN 55101.

Bureau of Quality Assurance, Department of Health and Family Services, 1 West Wilson Street, Suite 150, P.O. Box 7850, Madison, WI 53701–0309.

Louisiana Department of Health and Hospitals, Health Standards Section, 500 Laurel Street, Suite 100, Baton Rouge, LA 70801.

Texas Department of Human Services (TDHS), 701 West 51st Street, P.O. Box 149030, MC W–519, Austin, TX 78751.

Alabama Department of Public Health, Division of Health Care Facilities, 201 Monroe Street, Suite 840, P.O. Box 303017, Montgomery, AL 36104–3017.

Division of Emergency Medical Services, 570 East Woodrow Wilson Blvd., Third Floor A–300, Jackson, MS 39215.

State of New Jersey, Department of Health and Senior Services Long Term Care. Systems Development and Quality, 120 S Stockton Street, lower level, Trenton, NJ 08625.

Office of Health Facilities Licensing and Certification, LTC Residents Protection, Three Mill Road, Suite 308, Wilmington, DE 19806.

Colorado Department of Public Health and Environment, Health Facilities Division, HFD–a2, 4300 Cherry Creek Drive, South, Second Floor, Denver, CO 80246–1530.

Office of Health Quality, 2020 Carey Avenue, First Bank Building, 8th Floor, Cheyenne, WY 82002.

Department of Health & Human Services Division of Facility Services Licensure and Certification Section, 805 Briggs Drive, Raleigh, NC 27603.

SCDHEC, Division of Certification, 1777 Saint Julian Place, Suite 302, Columbia, SC 29204.

Seniors and People with Disabilities, 875 Union St.—4th Fl., Salem, OR 97310.

AASA—Division of Residential Services, 0B2 1115 North Washington, Olympia, WA 98503.

Myers and Stauffer, 6380 Flank Drive, Suite 100, Harrisburg, PA 17112.

DHHR, Management Information Services, 350 Capital Street, Room 206, Third Floor Computer Room, Charleston, WV 25301–3178.

Office of Regulatory Services, Georgia Department of Human Resources, 2 Peachtree Street North West, Suite 24, Atlanta, GA 30303–3167.

Management Information Systems, Agency for Health Care Administration, 2727 Mahan Dr, Fort Knox, Bldg 3, Room 100, MS9a, Tallahassee, FL 32308–5403.

Illinois Department of Public Aid, Division of Medical Programs, 201 South Grand Avenue, East, Prescott Bloom Bldg. 2nd floor, Springfield, IL 62763.

Indiana State Department of Health, 2 North Meridian Street, Indianapolis, IN 46204.

Cabinet for Health Services Office of Inspector General, 275 East Main Street 5E–A, Frankfurt, KY 40621.

Tennessee Department of Health, Division of Health Care Facilities, 426 5th Avenue, North, Cordell Hull Building, 1st Floor, Nashville, TN 37247–0508.

Massachusetts Department of Public Health, Division of Health Care Quality, 10 West Street, 5th floor, Boston, MA 02111.

Division of Licensing and Protection, 103 South Main Street, Ladd Hall room 898, Waterbury, VT 05671.

Missouri Department of Social Services, Division of Aging, 615 Howerton Court, Jefferson City, MO 65109.

Department of Human Services DMS/OLTC/ Reimbursement Unit, 700 Main, 4th Floor, PO Box 8059—Slot 407, Little Rock, AR 72203–8059.

Oklahoma State Department of Health, SHS, 1000 North East 10th Street, Oklahoma City, OK 73117–1299.

Myers & Stauffer Consulting Services, 4123 Southwest Gage Center Drive, Suite 200, Topeka, KS 66604.

Bureau of Licensure and Certification, 1550 East College Parkway, Suite 158, Carson City, NV 89706.

Arizona Department of Health Services, 1647 East Morten Ave., Suite 200, Phoenix, AZ 85020.

Virginia Department of Health, 1500 East Main Street, Room 211, Main Street Station, Richmond, VA 23219.

Department of Consumer and Regulatory Affairs, Service Facility Regulation Administration, 825 N Capitol Street NE., 2nd Floor LRA—Room 221, Washington, DC 20002.

Michigan Department of Community Health, 300 East Michigan, Chandler River Plaza Building, Lansing, MI 48933.

Ohio Department of Health, 246 N. High St., 3rd Floor, Columbus, OH 43215.

Dept of Human Services, 442 Civic Center Drive, Augusta, ME 04330.

Department of Health and Human Services, Office of Program Support, Office of Information Systems, 129 Pleasant Street, Brown Bldg., Concord, NH 03301–3857.

Office of Health Care Assurance, 601 Kamokila, RM 395, Kapolei, HI 96707.

South Dakota Department of Social Services, Office of Adult Services and Aging, 700 Governors Drive, Pierre, SD 57501.

California Department of Health Services, Licensing and Certification, 630 Bercut Dr. Suite B, Sacramento, CA 95814.

State of Maryland, Department of Health Care Quality, 55 Wade Avenue, Spring Grove

Center, Bland Bryant Bldg., Fourth Floor, Catonsville, MD 21228.

Department of Health and Human Services, Medicaid Division, P.O. Box 95026—301 Centennial Mall, South, 5th Floor, Lincoln, NE 68509.

DHHS Div of Med. Assistance Heath Facilities Licensing and Certification, 4730 Business Park Boulevard, Suite 18, Anchorage, AK 99503.

NYS Dept. of Health, Empire State Plaza, Concourse Room 148, Albany, NY 12237.

Virgin Islands, IFMC, 6000 Westown Parkway, West Des Moines, IA 50266.

Puerto Rico Department of Health, Assistant Secretariat for the Regulation and Accreditation of Health Facilities, Former Ruez Soler Hospital Road #2, Bayamon, PR 00959.

[FR Doc. 03–21444 Filed 8–21–03; 8:45 am]

BILLING CODE 4120–03–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Food and Drug Administration

[Docket No. 1999D–4577]

Guidance for Industry: Application of Current Statutory Authority to Nucleic Acid Testing of Pooled Plasma; Withdrawal of Draft Guidance

AGENCY: Food and Drug Administration, HHS.

ACTION: Notice; withdrawal.

SUMMARY: The Food and Drug Administration (FDA) is announcing the withdrawal of a draft guidance entitled ''Guidance for Industry: Application of Current Statutory Authority to Nucleic Acid Testing of Pooled Plasma'' dated November 1999, that was announced in the **Federal Register** on November 26, 1999. In the draft guidance, FDA sought public comment on the development and implementation of nucleic acid testing (NAT) for infectious diseases.

DATES: Effective September 22, 2003.

FOR FURTHER INFORMATION CONTACT: Astrid L. Szeto, Center for Biologics Evaluation and Research (HFM–17), Food and Drug Administration, 1401 Rockville Pike, Rockville, MD 20852–1448, 301–827–6210.

SUPPLEMENTARY INFORMATION: In a notice published in the **Federal Register** of November 26, 1999 (64 FR 66481), FDA announced the availability of a draft guidance entitled ''Guidance for Industry: Application of Current Statutory Authority to Nucleic Acid Testing of Pooled Plasma'' dated November 1999. This draft guidance responded to industry's request for guidance in the development and implementation of NAT of pooled plasma in further improving the safety of the nation's blood products. No NAT test kit manufacturers were licensed at that time. A number of manufacturers have subsequently been licensed for NAT, making the request for guidance in the development of NAT testing of pooled plasma for infectious agents now moot. This draft guidance is therefore being withdrawn as of September 22, 2003, because it is obsolete.

Dated: August 14, 2003.

William K. Hubbard,

Associate Commissioner for Policy and Planning.

[FR Doc. 03–21477 Filed 8–21–03; 8:45 am]

BILLING CODE 4160–01–S

DEPARTMENT OF THE INTERIOR

Fish and Wildlife Service

Receipt of Applications for Permit

AGENCY: Fish and Wildlife Service, Interior.

ACTION: Notice of Receipt of Applications for Permit.

SUMMARY: The public is invited to comment on the following applications to conduct certain activities with endangered species and/or marine mammals.

DATES: Written data, comments or requests must be received by September 22, 2003.

ADDRESSES: Documents and other information submitted with these applications are available for review, subject to the requirements of the Privacy Act and Freedom of Information Act, by any party who submits a written request for a copy of such documents within 30 days of the date of publication of this notice to: U.S. Fish and Wildlife Service, Division of Management Authority, 4401 North Fairfax Drive, Room 700, Arlington, Virginia 22203; fax 703/358–2281.

FOR FURTHER INFORMATION CONTACT: Division of Management Authority, telephone 703/358–2104.

SUPPLEMENTARY INFORMATION:

Endangered Species

The public is invited to comment on the following applications for a permit to conduct certain activities with endangered species. This notice is provided pursuant to Section 10(c) of the Endangered Species Act of 1973, *as amended* (16 U.S.C. 1531, *et seq.*). Written data, comments, or requests for copies of these complete applications should be submitted to the Director (address above).

Applicant: Miami Metrozoo, Miami, FL, PRT–069826.

The applicant requests a permit to export one male captive-born Baird's tapir (*Tapirus bairdii*) to the Parque Ecoarqueologico Xcaret, Mexico, for the purpose of enhancement of the survival of the species through captive propagation and conservation education.

Applicant: Yale University, New Haven, CT, PRT–072747.

The applicant requests a permit to import biological samples from sifaka (*Propithecus verreauxi verreauxi*) collected in the wild in Madagascar, for scientific research. This notification covers activities to be conducted by the applicant over a five-year period.

Applicant: Texas Memorial Museum, Austin, TX, PRT–072019.

The applicant requests a permit to import biological samples from Coahuilan box turtles (*Terrapene coahuila*) collected in the wild in Mexico, for scientific research. This notification covers activities to be conducted by the applicant over a five-year period.

Applicant: Susan C. Gardner, c/o U.S. Environmental Protection Agency, Cincinnati, OH, PRT–073075.

The applicant requests a permit to import samples and non-viable eggs obtained from green sea turtle (*Chelonia mydas*), olive ridley sea turtle (*Lepidochelys olivacea*), hawksbill sea turtle (*Eretmochelys imbricata*), and leather back sea turtle (*Dermochelys coriacea*), in Mexico, for the purpose of enhancement of the species through scientific research. This notification covers activities to be conducted by the applicant over a five year period.

Applicant: Dr. Lisa K.Yon, University of California, Davis, CA, PRT–075293.

The applicant requests a permit to import serum, urine, and fecal samples obtained from 6 bull Asian elephants (*Elephas maximus*) captive-held at the Ayutthaya Elephant Palace and Royal Kraal, Thailand, for the purpose of scientific research. This notification covers activities to be conducted by the applicant over a five-year period.

Applicant: Florida Museum of Natural History, Gainesville, FL, PRT–677336.

The applicant requests renewal of their permit to import export and re-export non-living museum specimens of endangered and threatened species of plants and animals previously accessioned into the applicant's collection for scientific research. This notification covers activities to be conducted by the applicant over a five-year period.

Applicant: Adam M. Vinatieri, North Attleboro, MA, PRT–075567.