

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