

CMS will only disclose the minimum personal data necessary to achieve the purpose of the MLNR-POS. CMS has the following policies and procedures concerning disclosures of information that will be maintained in the system. In general, disclosure of information from the SOR will be approved only for the minimum information necessary to accomplish the purpose of the disclosure after CMS:

1. Determines that the use or disclosure is consistent with the reason that the data are being collected; *e.g.*, tracking, reporting and accounting the disclosures made from all CMS systems of records as permitted by the Privacy Act and HIPAA.

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 individually, 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.

- d. Determines that the data are valid and reliable.

III. Proposed Routine Use Disclosures of Data in the System

A. Entities That May Receive Disclosures Under Routine Use

These routine uses specify circumstances, in addition to those provided by statute in the Privacy Act of 1974, under which CMS may release information from the MLNR-POS without the consent of the individual to whom such information pertains. Each proposed disclosure of information under these routine uses will be evaluated to ensure that the disclosure is legally permissible, including but not limited to ensuring that the purpose of the disclosure is compatible with the purpose for which the information was collected. CMS proposes to establish the following routine use disclosures of information maintained in the system:

1. To agency contractors, or consultants that have been contracted by the agency to assist in the performance of a service related to this system of records and that need to have access to the records in order to perform the activity.

CMS contemplates disclosing information under this routine use only in situations in which CMS may enter into a contractual or similar agreement with a third party to assist in accomplishing agency business 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.

2. 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.

Individuals sometimes request the help of a Member of Congress in resolving some 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.

3. 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.

Whenever CMS is involved in litigation, or occasionally when another party is involved in litigation and CMS's 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.

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 **Federal Register** 82462 as amended by 66 **Federal Register** 12434). 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 MLNR-POS will conform to applicable law and policy governing the privacy and security of Federal automated information systems. These include but are not limited to: the Privacy Act of 1974, 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 fully to guidance issued by the National Institute for Standards and Technology (NIST) in NIST Special Publication 800-18, "Guide for Developing Security Plans for Information Technology Systems." 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

Personnel having access to the system have been trained in Privacy Act 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