

sufficient to protect the confidentiality of the data and to prevent unauthorized access to the data. 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, the proper level of class user is assigned for each individual user level. This prevents unauthorized users from accessing and modifying critical data. The system database configuration 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;
- Quality Index 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; and
- Submitter class has read and write access to database objects, but no database administration privileges.

B. Physical Safeguards

All server sites will implement 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 CMS system:

Access to all servers is to be 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 is to require 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, which 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 (AIS) resources caused by fire, electricity, water and inadequate climate controls.

Protection applied to the workstations, servers and databases include:

- User Log-on—Authentication is to be performed by the Primary Domain Controller/Backup Domain Controller of the log-on domain.

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

- Hours of Operation—May be restricted by Windows NT. 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 to be determined and implemented at the agency level.

- Inactivity Lockout—Access to the NT workstation is to be automatically locked after a specified period of inactivity.

- Warnings—Legal notices and security warnings are to be displayed on all servers and workstations.

- Remote Access Security—Windows NT Remote Access Service (RAS) security handles resource access control. Access to NT resources is to be controlled for remote users in the same manner as local users, by utilizing Windows NT file and sharing permissions. Dial-in access can be granted or restricted on a user-by-user basis through the Windows NT RAS administration tool.

C. Procedural Safeguards

All automated systems must comply with Federal laws, guidance, and policies for information systems security. These include, but are not limited to: the Privacy Act of 1974; the Computer Security Act of 1987; OMB Circular A-130, revised; Information Resource Management Circular #10; HHS AIS Security Program; the CMS Information Systems Security Policy, Standards, and Guidelines Handbook; and other CMS systems security policies. Each automated information system should 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 New System on Individual Rights

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

CMS will monitor the collection and reporting of MLNR-POS data. MLNR-POS information is submitted to CMS through standard systems. CMS will use a variety of onsite and offsite edits and

audits to increase the accuracy of MLNR-POS data.

CMS will take precautionary measures (*see* item IV., above) to minimize the risks of unauthorized access to the records and the potential harm to individual privacy or other personal or property rights of patients whose data are maintained in the system. CMS will collect only that information necessary to perform the system's functions. In addition, CMS will make disclosure from the proposed system only with consent of the subject individual, or his/her legal representative, or in accordance with an applicable exception provision of the Privacy Act.

CMS, therefore, does not anticipate an unfavorable effect on individual privacy as a result of maintaining this system of records.

Dated: May 23, 2003.

Thomas A. Scully,
Administrator, Centers for Medicare & Medicaid Services.

09-70-0542

SYSTEM NAME:

MLN Registration and Product Ordering System, (MLNR-POS), HHS/CMS/CMM.

SECURITY CLASSIFICATION:

Level 3, Privacy Act Sensitive.

SYSTEM LOCATION:

HCFA Data Center, 7500 Security Boulevard, North Building, First Floor, Baltimore, Maryland 21244-1850. CMS contractors and agents at various locations.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

This system will contain the health care provider's first and last name, mailing address, provider type, facility type, telephone number, fax numbers and e-mail address. The data submission by the health care provider is voluntary. This system may collect social security number, provider number, UPIN number or contractor ID number.

CATEGORIES OF RECORDS IN THE SYSTEM:

This system will contain the health care provider's first and last name, mailing address, provider type, facility type, telephone number, fax numbers and e-mail address. The data submission by the health care provider is voluntary. This system may collect social security number, provider number, UPIN number or contractor ID number.