Chief Information Officer
Office of Information Services
Centers for Medicare & Medicaid Services

CMS Operational Policy for
Data Access Management

November 2004

TABLE OF CONTENTS

1. PURPOSE

This document establishes an operational policy for the training and access of enterprise data (including privacy-protected and non-privacy-protected data), that is used for non-operational functions at the Centers for Medicare & Medicaid Services (CMS).

2. BACKGROUND

The Enterprise Databases Group (EDG) within the Office of Information Services (OIS) maintains enterprise data structures on behalf of the Agency. These data structures are necessary for a variety of CMS transactional operations. CMS business components who need access to these data structures for sustained operations must work directly with the database maintainers in OIS/EDG to implement their transactions. Additionally, these enterprise databases are essential for non-operational functions, such as decision support, research, and policy activities. Non-operational users may need enterprise data only occasionally, and may be unfamiliar with the data and the data structures that are available to them. This policy addresses the specific training and access needs of non-operational CMS enterprise data users.

3. SCOPE

This operational policy applies to all CMS enterprise data users (including all CMS personnel and contractors), who request extracts of, or access to, non-operational CMS enterprise data.

4. OPERATIONAL POLICY

There are five levels of available training and access for CMS users of non-operational enterprise data, which are described below.

4.A Level I— Introduction to CMS Information Systems and Published Statistics

All CMS enterprise data users are required to complete an on-line training course that describes the enterprise information that is published on the CMS Intranet and/or Internet, as well as the information systems that are available at CMS.

This online training provides an overview of CMS published statistics, Part B Extract and Summary System (BESS), Health Care Information System (HCIS), Medicare Beneficiary Database (MBD) Mart/Reporting System, Medicaid data marts, Medicare and Medicaid Annual Person Summary data marts, Health Care Cost Report Information System (HCRIS) data, and any new data marts/reporting systems that are developed and maintained by OIS/EDG. Other CMS business components are also invited to participate in this online training to expose their information systems to CMS data users.

No approval or prerequisites are required for this online training.

To access the online training, the user must have a valid CMS User ID.

4.B Level II— CMS Statistical Information Systems

After completing Level I training, CMS enterprise data users will be introduced to the available CMS statistical and reporting systems, so that they can decide which systems are likely to meet their business needs.

Level II training will be available for all information systems included in the Level I overview. Some information system maintainers will provide courses, and others will provide one-on-one training as needed.

No approval is required for this Level II training.

Access to CMS statistical information systems will be based on prescribed RACF authority.

4.C Level III— CMS Statistical Information Systems Advanced Functions

For some CMS statistical information systems, OIS/EDG can give direct access to existing, partially summarized data. Level III access gives CMS enterprise data users access to data at a less-summarized level, and supports more customized queries. Data users requesting this level of access must meet with the EDG Access Approval Team to explain their business need prior to receiving Level III training and access approval.

OIS/EDG staff will conduct one-on-one training with CMS enterprise data users who have a demonstrated business need for the less-summarized data.

Prior to receiving Level III training/access, CMS enterprise data users must be certified at Level II and have received approval from the EDG Access Approval Team.

Access to CMS statistical information systems advanced functions will be granted to individual enterprise data users via the appropriate system owners/managers through RACF authority.

4.D Level IV— Controlled Access to Identifiable Data

Level IV access gives CMS enterprise data users access to identifiable data that is covered by the Privacy Act of 1974. OIS/EDG must control all access to privacy-protected data. CMS enterprise data users requesting Level IV access must follow established procedures in order to obtain access to privacy-protected data (see Attachment Section below).

The supervisor or project officer for the requesting CMS enterprise data user must meet with the EDG Access Approval Team to discuss their data needs. If it is determined that no available statistical or reporting system will meet the business needs, OIS/EDG will either provide the data requested using the most appropriate tool (e.g., Data Extract System (DESY), 100% TAP,

custom DB2 programming), or DESY training will be approved for the enterprise data user. New business requirements not satisfied by existing data marts or reporting systems will be identified by the EDG Access Approval Team and conveyed to the appropriate Integrated Data Team (IDT) within OIS/EDG for consideration in future data mart and reporting system development.

Level IV access requires mandatory DESY training on-site and/or remote training for Regional Office staff and contractors for National Claims History (NCH), National Medicare Utilization Database (NMUD), Medicare Beneficiary Database (MBD), Medicaid Statistical Information System (MSIS), and other data files available from DESY. Training includes data education, as well as the extract functions of the DESY tool.

At the conclusion of the training, an analyst from the EDG Access Approval Team will be assigned to each Level IV enterprise data user to continue training based on their individual requests. Users will work with the assigned OIS/EDG analyst to review their requests and the best method for extracting the data.

Prior to receiving Level IV training/access, CMS contractors and oversight agencies must have a signed Data Use Agreement (DUA). All Level IV enterprise data users must also have received prior Level I certification.

Controlled access to identifiable data will be based on prescribed RACF and DESY authority. DESY access will be turned off until each request developed by a new enterprise data user is reviewed and approved by the assigned OIS/EDG analyst.

4.E Level V— Direct Access to Identifiable Data

Level V access will be granted when the assigned analyst from the EDG Access Approval Team determines that a Level IV DESY user is fully trained.

Level V access requires one-on-one training with an analyst from the EDG Access Approval Team, annual training on new DESY functions, and annual training on the CMS information systems.

All Level V data users must have received prior Level IV certification and approval from an OIS/EDG analyst to be given full DESY access.

Direct access to identifiable (i.e., privacy-protected) data will be based on prescribed DESY authority or RACF authority to approved data stores. A signed DUA must also exist for CMS contractors and oversight agencies.

5. ROLES AND RESPONSIBILITIES

The following entities have responsibilities related to the implementation of this operational policy:

5.A. CMS Enterprise Data Users

CMS Enterprise Data Users are responsible for the following activities:

- Completing the appropriate levels of training and certification required in this operational policy in order to obtain appropriate access to CMS enterprise data; and
- Requesting access to identifiable (i.e., privacy-protected data) in accordance with the appropriate procedures (see Attachment Section below).

5.B. Office of Information Services (OIS)/ Enterprise Databases Group(EDG)

The OIS/EDG is responsible for the following activities:

- Developing and delivering training courses required for all levels of data access;
- Reviewing business needs of CMS Enterprise Data Users to determine appropriate data requirements and levels of access;
- Ensuring that CMS contractors and oversight agencies have signed Data Use Agreements in place prior to obtaining access to privacy-protected data;
- Serving as System Owner/Manager and System Maintainer for DESY, including managing the DESY tool to optimize data center resources and implementing changes to DESY to enforce data access policy requirements;
- Regularly reviewing DESY user access requests and educating CMS Enterprise Data Users on appropriate use of DESY; and
- Developing, implementing, and maintaining new data marts or statistical reports based on user requirements.

5.C. EDG Access Approval Team

The EDG Access Approval Team is comprised of senior data analysts and tool experts from within OIS/EDG, who advise CMS Enterprise Data Users on the availability of various data sources and the appropriate level of data access required to satisfy the user's business needs. The team also provides one-on-one training for advanced data mart access as approved, and mentoring for new DESY users. The analysts on the team give final approval for advancement to Level V.

5.D. System Owners/Managers

The System Owners/Managers of CMS' statistical information systems are responsible for granting RACF authority to individual CMS Enterprise Data Users for access to CMS statistical information systems advanced functions. The System Owner/Manager of DESY is responsible for granting RACF authority for access to the DESY tool.

5.E. System Maintainers

System Maintainers for some of CMS' information systems will be responsible for providing training courses, or one-on-one training as needed, to CMS Enterprise Data Users. The System Maintainer for DESY will be responsible for providing DESY training.

6. APPLICABLE LAWS/GUIDANCE

There are no laws or additional guidance applicable to this operational policy.

7. EFFECTIVE DATES

This operational policy becomes effective on the date that CMS' Chief Information Officer (CIO) signs it and remains in effect until officially superseded or cancelled by the CIO.

8. INFORMATION AND ASSISTANCE

Contact the Director of the Enterprise Databases Group (EDG) within the Office of Information Services (OIS) for further information regarding this operational policy.

9. APPROVED

/s/	11/8/04
Timothy P. Love	Date of Issuance
Chief Information Officer	

10. ATTACHMENTS

The following documents augment this operational policy:

- Procedure: Request for Privacy-Protected Data