Program Memorandum Intermediaries/Carriers

Department of Health & Human Services (DHHS)
Centers for Medicare & Medicaid Services (CMS)

Transmittal AB-02-172 Date: NOVEMBER 29, 2002

CHANGE REQUEST 2390

SUBJECT: Next Generation Desktop Data Center Connectivity – Security Information Clarification to Change Request 2079 (AB-02-073) Dated May 16, 2002

This document provides additional clarification to Change Request 2079, which outlines CMS expectations for implementation of the Medicare Customer Service Center (MCSC) Next Generation Desktop (NGD).

SECURITY ISSUES

Call and Data Center

NGD retrieves data from systems, such as the CMS Enrollment Database (EDB) and the SSA Master Beneficiary Record (MBR). These systems are Privacy Act protected and require high levels of security. Data and Call Centers are required to follow strict security controls in their data center implementation to segregate CMS data from other business data and to safeguard the confidentiality, integrity and availability of such data.

NGD Network Traffic and Overview

For MCSC NGD implementation, connectivity must be established between Siebel NGD and SNA (System Network Architecture) servers, the Medicare Data Communications Network (MDCN) and the Medicare Call Center's servicing data center. Currently, the Siebel NGD and SNA gateway servers reside at the AdminaStar Federal Data Center in Louisville, Kentucky.

A Customer Service Representative (CSR), as a NGD user located at the Medicare Call Center, uses a browser-based, thin client with zero footprint to access the Siebel NGD servers. All communications between client and server travel via the MDCN, provided by AT&T Global Network Services (AGNS). This configuration establishes a **Virtual Private Network** (VPN) connection between the Louisville Data Center's NGD Complex and each Data Center.

When the Siebel NGD application requests Medicare shared claims processing systems information for an NGD user, the NGD systems' Integration Server acts on behalf of the NGD user and utilizes a CICS transaction-based approach to retrieve the requested information. This SNA connection communicates directly with the Medicare shared claims processing systems (MCS, VMS, FISS) via the MDCN, to process the NGD users' information request.

NGD update requests to Medicare shared claims processing systems are limited to users within the local call center, as controlled by their specific data center site security. Therefore, updates are allowed only to native users. **Non-native call center NGD users (e.g. other Medicare Call Centers) will have read-only access to the specific data center's Medicare systems as described in the Mainframe ID's paragraph below**. Memorandums of understanding between the data center and call center contractors will be needed prior to NGD's authorization (or capability) to update Medicare shared claims processing systems that are not native to the NGD user. If this non-native update capability becomes necessary, CMS will work with call center contractors to establish these memorandums of understanding.

Mainframe ID's Clarification

The Siebel application identifies the information's requester and determines the source required to fulfill the information request. This information is passed to the Integration Server, which establishes a session between NGD Data Center and the source Data Center. The Integration Server uses an established Logical Unit (LU) connection from available LU session pools. Each Data Center will be assigned a specific number of LU session IDs, which will be assigned and controlled by AGNS.

The session pool concept is referred to as Master ID since only a limited number of sessions are available for a larger number of users sessions. Master IDs are used by NGD Integration Servers, which acts in behalf of NGD users, to access the source Data Center's mainframe. Master IDs have been successfully implemented within other CMS applications with similar large user base and technical requirements. It is important to note that allowing NGD users read-only access to other Medicare contractors databases is not a new idea, and in theory the NGD read-only access is not too different than the shared access that all Medicare contractors have to the Common Working File (CWF).

The Data Center's System Administrators restricts and controls access to the shared claims processing systems housed at their data center, thus protecting the Government's Medicare claims information that they have been entrusted to maintain. **It is the Data and Call Centers System Administrators' responsibility to establish, add, and maintain the NGD-provided LU sessions and Master IDs on the mainframe's security software for NGD access as needed for development, validation, training, and production.** The benefit of establishing and maintaining a limited number of LU IDs and Master IDs for each Call Center, versus establishing individual accounts for each NGD user, results in reduced administrative tasks and costs.

NGD Security Responsibilities
The NGD Contractor (currently AdminaStar Federal) is responsible for the security controls within NGD. **It is National NGD Security Administrators' responsibility to establish, add maintain, and track the AGNS-provided LU sessions and Master Ids for all Medicare contractors on the applicable NGD software, (e.g., Siebel server, Jacada server, etc.).** The NGD software is developed to enable each Call Center to grant security access to its files, and will only retrieve/display data defined within the security access granted. Security tests have been developed to ensure access controls mechanisms are in place and operating as intended.

Stringent controls and monitoring processes will be in place to ensure that only assigned personnel gain access to the range of IDs assigned to their Center. Those transactions will be performed in NGD's authentication servers within a secured environment.

The NGD system generates transaction logs with information to fulfill user traceability requirements. The Siebel server, Integration server, and CICS/SNA gateway logs will document the transactions being performed, who performed them, when they were performed, what User ID and what LU session, host, and system were used to perform the transaction. This logging supports the use of Master IDs within the NGD, providing individual accountability for NGD users. Auditing will be performed within the NGD network and will provide a trace mechanism for the Medicare shared claims processing systems to validate users.

Security Oversight
Oversight and separation of duties for NGD security will be accomplished by:

(1) Establishing System Administrators for Call and Data Centers, when applicable, with access only to the range of IDs designated for their Center;

(2) Establishing a National NGD Security Administrator responsible for establishing user IDs and granting security access to Call and Data Center's System Administrators; and

(3) Designating a third-party to audit security functions and logs, including the National NGD Security Administrator.

These instructions should be implemented within your current operating budget. FY 2003 costs should be included in your budget request.

The effective date for this Program Memorandum (PM) is November 26, 2002.

The implementation date for this PM is December 13, 2002.

This PM may be discarded after November 26, 2003.

If you have any questions, contact Stephanie Bojanowski at sbojanowski@cms.hhs.gov or Carol Davis at cdavis2@cms.hhs.gov