Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

CMS Security Whitepaper:

Fee-for-Service Application User Access Recertification Whitepaper

FINAL
Version 2.0
March 08, 2009

(This Page Intentionally Blank)

SUMMARY OF CHANGES IN *FEE-FOR-SERVICE APPLICATION USER ACCESS RECERTIFICATION* WHITEPAPER, VERSION 2.0

1) Converted baseline version dated January 24 2008 to updated CMS style format.
2) Moved Introduction, from before Table of Contents to after into new Section 1.
3) Moved text from Introduction into new Section 1.1, Scope.
4) Moved text from former Section 1, Background, into new Section 1.2, Background.
5) Added subsection numbering to Section 3, Components of Effective Application User Access Registration.
6) Added subsection numbering to Section 4, Other Controls to Consider.
7) Removed former Appendix A CSRs and added pointer to new CMSRs.
8) Changed CSR glossary term in Appendix B to CMSR.
9) Added titles to Figure 1, 2, 3, 4, 5, 6, and 7; and Table 1, 2, and 3 in Appendix C.
10) Added titles to Figure 8 and 9, and Table 4 and 5 in Appendix D.
11) Added titles to Figure 10 and Table 6 in Appendix E.
12) Added titles to Figure 11, 12, and 13; and Table 7 in Appendix F.
13) Updated the Appendix A CMSR reference.

SUMMARY OF CHANGES IN *FEE-FOR-SERVICE APPLICATION USER ACCESS RECERTIFICATION* WHITEPAPER, VERSION 1.0

1) Baseline Version 1.0.

(This Page Intentionally Blank)

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 INTRODUCTION

1.1 SCOPE

This white paper was developed by PricewaterhouseCoopers LLP (PwC) for the Centers for Medicare and Medicaid Services (CMS). This document is one of a number of white papers issued by CMS management to assist with the proper understanding and implementation of key security controls around CMS' data and information systems environment.

The intended audience of this paper however, extends beyond CMS management and staff to include all CMS business partners. In this context, a CMS business partner is any private or public sector organization which provides services to this agency. These business partners include, but are not limited to: Medicare Carriers, Fiscal Intermediaries (FIs), Durable Medical Equipment Medicare Administrative Contractors (DME MACs), standard claims processing system maintainers, Regional Laboratory Carriers, claims processing data centers, A/B Medicare Administrative Contractors (MAC), Enterprise Data Centers (EDC), and other partners as directed.

In 2007, a review of access recertification processes for claims processing systems used by the CMS Fee for Service contractors was conducted. The review found that FIs, Carriers, DME MACs, and A/B MACs were performing periodic user access recertification, although many lacked strong user access recertification processes to ensure that user access rights within the claims processing systems were appropriate. National Institutes of Standards and Technology (NIST) Special Publication (SP) 800-12, An Introduction to Computer Security: The NIST Handbook, Section 10.2.2 states, "From time to time, it is necessary to review user account management on a system. Within the area of user access issues, such reviews may examine the levels of access each individual has, conformity with the concept of least privilege, whether all accounts are still active, whether management authorizations are up-to-date, whether required training has been completed, and so forth."

Security settings enabled by the claims processing systems allow users to perform one or more job functions such as claims entry, claims adjudication, accounting, customer service, security administration, systems programming, and system support. The standard claims processing systems include: Fiscal Intermediary Shared System (FISS), Multi-Carrier System (MCS), and ViPS Medicare System (VMS). Lack of periodic recertification of user access rights introduces the possibility that users who retain access rights outside their job function may inappropriately view or modify sensitive Medicare claims data. The recertification of user access rights on a periodic basis helps to ensure that access to Medicare claims data is restricted only to those users who should have such access, thus ensuring that the concept of least privilege is supported. Through the implementation of an effective user access recertification process, the likelihood of unauthorized changes, whether intentional or unintentional, to Medicare claims data can be significantly decreased.

This white paper has been created to assist CMS Business Partners in determining the appropriateness of controls over Fee for Service application user access recertification. Topics presented within this document include the following:

- Background of application user access recertification;
- Results of the review of Fee for Service application user access recertification;
- Components of effective application user access recertification; and
- Additional controls to consider during the implementation of a recertification process.

This paper serves to provide a foundation for CMS management and business partners to ensure that key controls pertaining to fee for service application access recertification are fully incorporated into CMS' control environment.

1.1 BACKGROUND

A fundamental requirement of any secure application is to provide controlled access to its resources. Access control is a mechanism that is used to limit access to only trusted entities that have a business need to use a particular resource. Controlling access helps ensure the confidentiality, integrity, and availability of the application resources; in this case, Medicare claims data.

- **Confidentiality** makes certain that information is disclosed only to authorized individuals. Authorized individuals are determined based upon company policy, regulations, and the principle of need-to-know. The principle of need-to-know is a concept where access to information is granted only when it is required to complete a job duty or task.
- **Integrity** is the reliability of information that it is correct, consistent, and protected from unauthorized use or modification. One safeguard for protecting integrity is the use of the least-privileged principle. The least-privileged principle makes certain that users only have the necessary permissions to perform their job duties, and nothing more.
- **Availability** is the accessibility of system resources when needed and by those who need them.

There are numerous controls that Medicare contractors can implement to control access to Medicare claims data within the Fee for Service applications. This document describes the control of user access recertification.

Management should ensure an appropriate balance of controls exists to ensure there is less than a remote likelihood that a misstatement of the financial statements could arise from unauthorized or erroneous changes to Medicare data via unauthorized access. In previous audits, it was noted that contractors had access to system functions or features outside their job responsibilities. During the Audit of the CMS Financial Statements for Fiscal Year (FY) 2007, an examination of the performance and effectiveness of user access recertification was performed. The evaluation noted five key areas for which Carriers, FIs, DME MACs, and A/B MACs lacked pervasive controls for access recertification:

- Policies and procedures;
- Standard profiles or templates for each job function;

- Documentation to support deviations from the standard profile or template;
- Appropriate approval; and
- Proper segregation of duties.

As a result of the identification of these five key areas during the Audit, it was recommended that Medicare contractors evaluate the appropriateness and need for user's access rights within the standard claims processing systems. This should include an evaluation of the environment, an assessment of the risks associated with all access rights, and an assessment of the controls presently in place. Establishing controls over the addition, deletion, or modification of access rights through the recertification process is critical to ensure the confidentiality, integrity, and availability of sensitive Medicare data.

2 SUMMARY OF RESULTS OF APPLICATION USER ACCESS RECERTIFICATION REVIEW

The Chief Financial Officers Act Audit of the U.S. Department of Health and Human Services included a review of CMS Financial Statements for FY 2007. During the Audit, Fee for Service application user access recertification procedures and controls were reviewed. The examination consisted of the following procedures for selected Carriers, Fiscal Intermediaries, and MACs, specific to the claims processing systems which were in use:

- Inspected access recertification procedures;
- Inspected profiles/templates used to assign access;
- Inspected access reports (e.g., Operator Control File, Clerk File, VSEC File);
- Inspected evidence of access recertification for a selection of Fee for Service application users; and
- Inspected evidence of key access recertification elements, including appropriate approval, documentation, and documented approval of variances.

The evaluation noted many of the same issues across all Medicare contractors, regardless of the application being used. The following are areas in which issues were noted during the evaluation, as well as evaluations performed during previous audits:

- **Policies and procedures:** Formal documented application user access recertification procedures did not exist; policies and procedures were in draft and had not been approved by management and incorporated into the organization; high level procedures did not provide sufficient details including, but not limited to: frequency of recertification, review of both access to the application and access within the application, a comparison of actual access to predetermined templates, periodic review of role based templates, documentation requirements, and approvals for deviations.
- **Standard templates for each job function:** Templates for job functions were not periodically reviewed for appropriateness; actual user access deviated from pre-determined

template; and, users were not assigned to specific roles/templates therefore access was set at the individual level.

- **Approval:** Users were not recertified by their immediate supervisor and users were recertifying their own access.
- **Segregation of duties:** Users had been granted access outside their pre-determined template and templates were not set up in accordance with the concept of least privilege needed to perform job responsibilities.

Overall, Carriers, Fiscal Intermediaries, and MACs did not have strong application user recertification processes in place. In most cases, Medicare contractors had recertification processes in place; however, contractors were not performing reviews which encompassed all major components of effective recertification. In other cases, formal, documented policies and procedures had not been developed or implemented, or documentation maintained to support recertification was insufficient.

3 COMPONENTS OF EFFECTIVE APPLICATION USER ACCESS RECERTIFICATION

The effectiveness of access controls can be impacted by factors such as employee turnover, changes in department, promotions, unintentional actions, or intentional unauthorized actions. For these reasons, access authorizations should be evaluated regularly to make certain the ongoing validity of users' access rights.

The following sections discuss some of the key components for incorporating an application user access recertification process into an organization.

3.1 DOCUMENTED POLICIES AND PROCEDURES

Contractors should either adopt or enhance an existing access control policy to initiate the review of user access rights to the Fee for Service applications. This policy should set the tone from management that user access rights will be reviewed and recertified on a periodic basis. The policy may also provide applicable standards, roles and responsibilities, possible consequences for non-compliance, and additional documentation for reference. The overarching policy should be put into practice through detailed procedures which provide guidance throughout the entire process. Recertification procedures may be created and implemented for each Fee for Service application, or management may institute a procedure which is inclusive of all Fee for Service applications used. Regardless of the method chosen, application recertification procedures should be clear and concise and should guide data owners, supervisors, managers, security personnel, and other applicable parties through each component of the recertification process.

Both policies and procedures should be reviewed annually or upon change to the process by appropriate parties to make certain they reflect the current environment. In addition, updates to the policies and procedures should be communicated to the affected parties.

The remainder of the topics in this section will discuss key components of an application user access recertification process. These elements should be documented in the policies and procedures discussed above. The sections below will also provide details related to the FISS, MCS, and VMS applications.

3.1 ROLE-BASED ACCESS CONTROL

Role-based access control is the method of defining, managing, and enforcing access control through the use of intermediary components (e.g. roles) between end-users and permission assignments. Through roles, the number of permission relationships that must be managed is greatly reduced. Permissions are assigned to roles instead of being assigned directly to end users. The reduction in the administration of permissions to be managed is the key benefit and why role based access should be implemented.

NIST SP 800-12, Section 17.1.2 states, "Access to information may also be controlled by the job assignment or function (i.e., the role) of the user who is seeking access…Access rights are grouped by role name, and the use of resources is restricted to individuals authorized to assume the associated role. The use of roles can be a very effective way of providing access control. The process of defining roles should be based on a thorough analysis of how an organization operates and should include input from a wide spectrum of users in an organization."

For the Fee for Service applications, roles should represent a user's job functional responsibilities (claims operator, customer service representative, security administrator, etc.). Templates should be created for each role, and should be based on each Fee for Service application's mechanism for controlling and restricting access. Data owners and managers should assess the access capabilities needed by users to perform their day-to-day job functions, and should be held responsible for the creation, periodic review, revisions, and ownership of roles and templates. Data owners and managers should establish roles such that the need for deviations from those templates should be unusual and limited. When deviations from the templates are necessary, those variances should be documented as a deviation to a defined profile.

The access control mechanism for each Fee for Service application is described below.

3.1.1 FISCAL INTERMEDIARY STANDARD SYSTEM (FISS)

Templates should be created by FIs and A/B MACs that include all functions defined in the Operator Control File. The Operator Control File consists of 7 screens which provide for transaction security access and allow the administrator to type the appropriate access level needed for each function. Valid transaction security access values for the functions are as follows:

- **Y**: Enter, update or inquire
- **I**: Inquire only
- **N** (or blank): No access allowed

The appropriate value (Y, I, or N) for each function in regards to the specific role should be documented in each template. FISS users should be aligned with the template that accurately reflects their role; and their access within FISS should match that of the template. A list of users associated with each role and template should be maintained and regularly updated by data owners and managers.

Refer to Appendix C for Operator Control File screen examples and descriptions of the Operator Control File functions.

3.1.1 MULTI-CARRIER SYSTEM (MCS)

Templates should be created by Carriers and A/B MACs which include all functions defined in the Clerk Record Update Screen. The Clerk Record Update Screen consists of 2 screens which define the security level settings for each clerk. Valid values for the functions are as follows:

- **Y**: Enter, update or inquire
- **U**: Update only
- **I**: Inquiry only
- **N**: No access allowed

The appropriate value (Y, U, I, or N) for each function in each specific role should be documented in the templates. MCS users should be aligned with the template that accurately reflects their role; and their access should match that of the template. A list of users associated with each role and template should be maintained and regularly updated by data owners and managers.

Refer to Appendix D for Clerk Record Update Screen examples and descriptions of the Clerk Record Update Screen functions.

3.1.1 VIPS MEDICARE SYSTEM (VMS)

Templates should be created by DME MACs which include all security switches defined in the Security Express Screen. The Security Express Screens are accessible via the VMS Security system (VSEC). The Security Express Screen lists the security level switch settings for each user. Valid security switch settings are as follows:

- **Y**: Allow access
- **N**: Deny access

VMS uses a hierarchal security structure that consists of three tiers: Corporate Security Officer, Department Security Officer, and user/operator. Because of its three-tiered security structure, VMS contains features that allow for role-based access control within the system.

The Corporate Security Officer is the highest level of security administration, and is responsible for adding departments and Department Security Officers. The Corporate Security Officer can

set security switches for departments, transfer users to other departments, and perform all of the Department Security Officer tasks described below.

Department Security Officers are responsible for adding the job functions for their department and assigning the appropriate security switch settings for the job function. Department Security Officers add users and have the ability to assign the user to a job function. By doing so, the user inherits the security switch settings defined by the job function thereby instituting role-based access control. Other tasks the Department Security Officer can perform include: updating user information, setting individual user ID switches, deleting users, transferring a user to another department, adding/deleting provider access to VMS, deleting provider access, and requesting security reports.

Users/operators at the third tier may view their security switch settings and ID information only. A list of users/operators associated with each role and template should be maintained and regularly updated by data owners and managers.

Refer to Appendix E for Security Express Screen examples and descriptions of the VMS security switches.

3.2 CONTROLS OVER SPECIAL/UNIQUE ACCESS

Medicare Contractors should avoid assigning access rights to users outside of their predetermined template. However, in certain circumstances, deviation(s) from a user's template may be necessary. Deviations from templates should be limited to those who have an appropriate business justification. Data owners and managers should evaluate whether elevated access rights are required for the user to perform their daily job duties. Medicare Contractors should have business justifications formally documented and approved by management for instances where a user requires such deviation(s). Specific procedures should be developed that ensure proper review and approval for assigning access outside of the predetermined templates.

For purposes of short-term or temporary elevated access (e.g., backup duties), Medicare Contractors should make certain that standing deviated access rights are not provided. NIST SP 800-12, Section 10.2.4 states, "Users often are required to perform duties outside their normal scope during the absence of others. This requires additional access authorizations. Although necessary, such extra access authorizations should be granted sparingly and monitored carefully, consistent with the need to maintain separation of duties for internal control purposes. Also, they should be removed promptly when no longer required." In such instances, Medicare Contractors should develop a process and documented procedure for obtaining temporary elevated access. This process and procedure should include:

- A formal request for access
- Details on the security settings to be altered
- Business justification
- Documented management approval
- Documented termination date for elevated access

- The removal of access on the specified termination date

Prior to approving a temporary access request, management should evaluate the reasonableness of the business justification and the reasonableness of the duration of time in which the access is requested. Management should also make certain that elevated access rights are removed as soon as the task or job at hand is completed.

Data owners, supervisors, and managers should consider creating an additional role and template if multiple users require the same deviation(s).

3.3 AN EFFECTIVE ACCESS RECERTIFICATION PROCESS

As described above, the components of an effective application user access recertification process include documented policies and procedures, role based access controls, and controls surrounding special or unique access. User access to the Fee for Service applications should be recertified, at a minimum, on an annual basis to make certain that users' access rights are valid and have not deviated from their predetermined templates.

The Fee for Service application user access recertification process should begin with an assessment of existing roles and templates, whether they are maintained in paper or electronic format. Data owners and managers should consider the following questions when performing this assessment:

- Is the role valid?
- Are the security settings associated with the role valid?
- Is it necessary to create new roles and templates?

Roles should be re-authorized and formally approved by management. Any necessary changes should be communicated to security administration.

The next step in performing application recertification is the evaluation of the user. A complete list of users to the Fee for Service applications should be generated at the time of recertification. The reports listing each user and their access rights for the Fee for Service applications are as follows:

- FISS - Operator Control File (FSSOPER);
- MCS - Clerk File Security Report (H99RCRCF); and
- VMS - Operator Security List Report (SE5502) and Operator Security Detail Report (SE5501)

Refer to Appendix F for example security reports and instructions for generating the reports.

Questions to consider for each user are the following:

- Does the user still need access to the application? Is the user an active employee or has the user been transferred/terminated?

- Has the user been assigned to a template? Does the assigned template accurately reflect the user's role?

Management should perform a manual comparison of the access rights defined in the user's template to the user's actual assigned access rights using the Fee for Service security reports described above. Management should investigate any deviations and make certain that documented business justification and approval of deviations exist. An evaluation of deviations from templates should be also included in the recertification process. Any needed changes should be communicated to security administration.

Finally, security administration should reproduce the Fee for Service application security reports and distribute them to management after all requests for revisions, additions, or deletion of roles, templates, and user access rights have been processed and completed. Management should review the reports and confirm that the changes made by security administration were accurate.

All documentation and approvals supporting the recertification of templates and users generated as a result of the recertification should be maintained. Documentation should be retained for a minimum of one year and should be readily available for audit purposes.

4 OTHER CONTROLS TO CONSIDER

In addition to periodic application user access recertification, Medicare Contractors should make certain that additional access controls are in place to reduce the risk of unauthorized disclosure or changes to Medicare data. Together all access control mechanisms, when implemented effectively, help to safeguard the confidentiality, integrity, and availability of Medicare data.

The following sections discuss some of the additional access controls that Medicare Contractors should consider.

4.1 ACCESS AUTHORIZATION AND RECERTIFICATION OF EXTERNAL USERS

Medicare Contractors should exercise control over the external users who are accessing their systems. Lack of strong control over external user access to the Fee for Service applications increases the possibility that sensitive Medicare information is disclosed, and false claims may be entered. Both the FISS and VMS Fee for Service applications have features which allow external users, typically providers, to access the system. FISS allows Direct Data Entry (DDE) whereby external users directly key in claims transactions into the FISS system. VMS allows providers to view the status of a claim via its PINQ transaction. PINQ is simply a status inquiry transaction; therefore providers do not have the authority to enter, make modifications, or make updates to claims.

It is important that Medicare Contractors first adopt a process for granting access to external users. This process should include a documented procedure, formal documented request for access, role(s) and template(s) for external users, and a formal approval of access by management. Separate user IDs and passwords should be generated for each external user.

Medicare Contractors should implement an external user application access recertification process similar to the process for recertifying internal users. An effective external user application recertification process includes a documented policy and procedure, recertification of the external user template by the Medicare Contractor, and a recertification of the external user by the external party.

Medicare Contractors should obtain confirmation from the external user's supervisor or manager. A formal letter should be sent to external entities stating the purpose of the recertification, a list of IDs and names of staff belonging to the external entity with access to the application(s), and a request for confirmation by a given date that the access is needed.

The external parties should consider the following questions when performing the assessment:

- Is the external user is still an active employee of the external entity?
- Does the external user require access to the Fee for Service application to perform their day-to-day job?

After confirmation has been received from the external entity, any necessary changes should be communicated to security administration. User IDs should be revoked if confirmation is not received from the external entity on the specified date. After all requests for modifications or removal of access have been completed by security administration, security administration should generate the Fee for Service application security reports and distribute the reports to management. Management should review the reports to make certain that changes made by security administration were accurate.

All documentation and confirmations supporting the recertification of external users generated as a result of the recertification should be maintained. Documentation should be retained for a minimum of one year and should be readily available for audit purposes.

4.1 ACCESS ADMINISTRATION

It is important that Medicare Contractors carefully manage controls over granting access, revising access, and removing access to the Fee for Service applications. Strong security administration practices also help to simplify the periodic recertification process.

Policies over granting, revising, and removing access should be included in the security policy. Procedures on the administration of access should be formally documented, clear and concise, and should be periodically reviewed and updated.

4.1.1 INITIAL (NEW USER) ACCESS

The initial request for access to the Fee for Service application(s) should be controlled through the use of a formal Access Request Form. NIST SP 800-12, Section 10.2.2 states, "User account management typically begins with a request from the user's supervisor to the system manager for a system account. If a user is to have access to a particular application, this request may be sent through the application manager to the system manager. This will ensure that the systems office receives formal approval from the 'application manager' for the employee to be given access.

The request will normally state the level of access to be granted, perhaps by function or by specifying a particular user profile. (Often when more than one employee is doing the same job, a 'profile' of permitted authorizations is created.)"

An Access Request Form may be in paper or electronic formation and should include, at a minimum:

- Name of the user;
- Name of the requester;
- Date requested;
- Fee for Service application(s) to be accessed;
- Regions/instances to be accessed;
- Role/template for the new user; and
- Approval from an authorized approver.

Access Request Forms are typically completed by the user's supervisor or manager. Security administration should not process new access requests unless the Access Request Form is complete and contains a digital or electronic approval from an authorized approver. A list of authorized approvers should be maintained and regularly updated by security administration.

In addition, it is essential that management and/or security administration confirm that the new user has completed mandatory Security Awareness Training prior to the granting of Fee for Service application access. For example, management may include a copy of the user's Security Awareness Training completion certificate to the Access Request Form, or security administration may validate completion through requested training reports from the education/training department. Regardless of the method chosen, it is essential that new users understand their responsibilities and expected behaviors prior to accessing Medicare data.

4.1.1 CHANGE IN ACCESS

Any changes in access requirements to the applications due to circumstances such as promotions, department transfers, change in job responsibilities, etc. should be controlled through formal Transfer Request Forms. NIST SP 800-12, Section 10.2.4 states, "Permanent changes are usually necessary when employees change positions within an organization. In this case, the process of granting account authorizations will occur again. At this time, however, is it also important that access authorizations of the prior position be removed. Many instances of 'authorization creep' have occurred with employees continuing to maintain access rights for previously held positions within an organization. This practice is inconsistent with the principle of least privilege." Transfer Request Forms may be in paper or electronic format and should include, at a minimum:

- Name of user and application ID(s);
- Name of requestor;

- Date the transfer is effective;
- Old role/template;
- New role/template; and
- Approval from an authorized approver.

Transfer Request Forms should be completed by the user's new supervisor or manager and approved by an authorized approver.

4.1.1 REMOVAL OF ACCESS

A terminated individual should have application access rights removed as soon as possible. Terminated users, especially those who leave involuntarily, who continue to have access to the Fee for Service applications pose as a threat to the confidentiality, availability and integrity of Medicare data. NIST SP 800-12, Section 10.2.5.2 states, "Given the potential for adverse consequences, security specialists routinely recommend that system access be terminated as quickly as possible in such situations."

It is important that security administration is notified immediately when a user is terminated. Notification should be provided by human resources or management. Regardless, responsibility for notification should be documented in termination procedures. Notification should be provided to security administration in a formal Termination Request Form which should include, at a minimum:

- Name and application ID(s) of the terminated individual;
- Effective date of termination;
- Application(s) in which access is to be removed; and
- Approval from an authorized approver.

Best practices suggest that access to the Fee for Service applications be removed after an employee has ceased employment. Compensating controls, such as the review by security administration of weekly human resources termination reports also aid in the strengthening of termination controls.

4.2 REMOVAL OF INACTIVE USERS

Medicare Contractors should make certain that inactive user accounts, both internal and external, are monitored and disabled after an organization-defined period of time. Accounts should be terminated if not necessary for a user to perform their day-to-day responsibilities. Procedures for the monitoring and disabling of inactive user accounts should be formally documented and periodically reviewed for appropriateness.

Best practices suggest that user accounts should be automatically disabled or revoked after thirty days of inactivity. The user and user's manager should be notified of the disabled accounts. If

the account is still needed, management should document business justification and provide it to security administration prior to resetting the account.

4.3 SEGREGATION OF DUTIES - LEAST PRIVILEGE

Segregation of duties is a concept that splits business operations into separate tasks so that one individual is not allowed to complete the business operation alone. Segregation of duties is one of the most fundamental principles of good internal control. When properly implemented, it reduces or eliminates the possibility that a single person can perform two or more functions in such a way that error or misappropriation could occur. These errors may not be detected in a timely manner and in the normal course of business processes.

For example, it is not desirable to grant privileges of claims entry and Common Working File (CWF)[1] bypass capability to the same person. Assigning both capabilities to the same individual can lead to conflicts of interest. When a person who entered a claim may have the claim be approved for payment without validation from CWF, assurance over data integrity is reduced.

When addressing role based access control within the Fee for Service applications, segregation of duty conflicts must be identified and addressed to make certain that a user is not assigned a combination of application roles that result in an unacceptable level of risk. Segregation of duties is considered valuable in deterring inappropriate activity (i.e. fraud) and assigning accountability within an organization. The use of role based access control can aid in a better evaluation of segregation of duties requirements and apply mechanisms to assist in monitoring and enforcing segregation of duty policies.

When establishing roles for users of application, data owners and managers must make certain that the concept of least privilege is supported. As stated in the Introduction of this document, the least privileged principle is the concept that a user is granted only the accesses needed to perform their official duties. NIST SP 800-12, Section 10.2.1 states, “It is essential to realize that access and authorization administration is a continuing process. New user accounts are added while others are deleted. Permissions change: sometimes permanently, sometimes temporarily. New applications are added, upgraded, and removed. Tracking this information to keep it up to date is not easy, but is necessary to allow users access to only those functions necessary to accomplish their assigned responsibilities thereby helping to maintain the principle of least privilege.”

Strong control over segregation of duties may be difficult for smaller organizations to implement. When lacking strong segregation of duties, Medicare Contractors must make certain that appropriate compensating controls are implemented. Compensating controls can include, but are not limited to: audit trails; reconciliation; exception reporting; supervisory reviews; transaction logs; and independent reviews.

[1] Claims which have passed the Fee for Service application edit checks are sent to CWF. CWF Hosts return approvals for payment, rejects, or adjustments. Information on CWF was obtained from Chapter 27, Section 10 of the Medicare Claims Processing Manual Revision R1332CP (http://www.cms.hhs.gov/manuals/downloads/clm104c27.pdf)

5 CONCLUSION

The Fee for Service applications are significant components to the processing of Medicare claims. CMS, FIs, Carriers, MACs, providers, and beneficiaries are all impacted by such applications. Thus, controls over users who have access to the Fee for Service applications, as well as controls over user access privileges within the applications, are essential to maintaining the confidentiality, integrity, and availability of Medicare data. The periodic recertification of access decreases the risk of unauthorized disclosure or modifications to Medicare data. Using the guidance provided in this document, FIs, Carriers, MACs, and other business partners as directed will be able to build strong controls around Fee for Service application user access.

APPENDIX A - CMS MINIMUM SECURITY REQUIREMENTS (CMSRs)

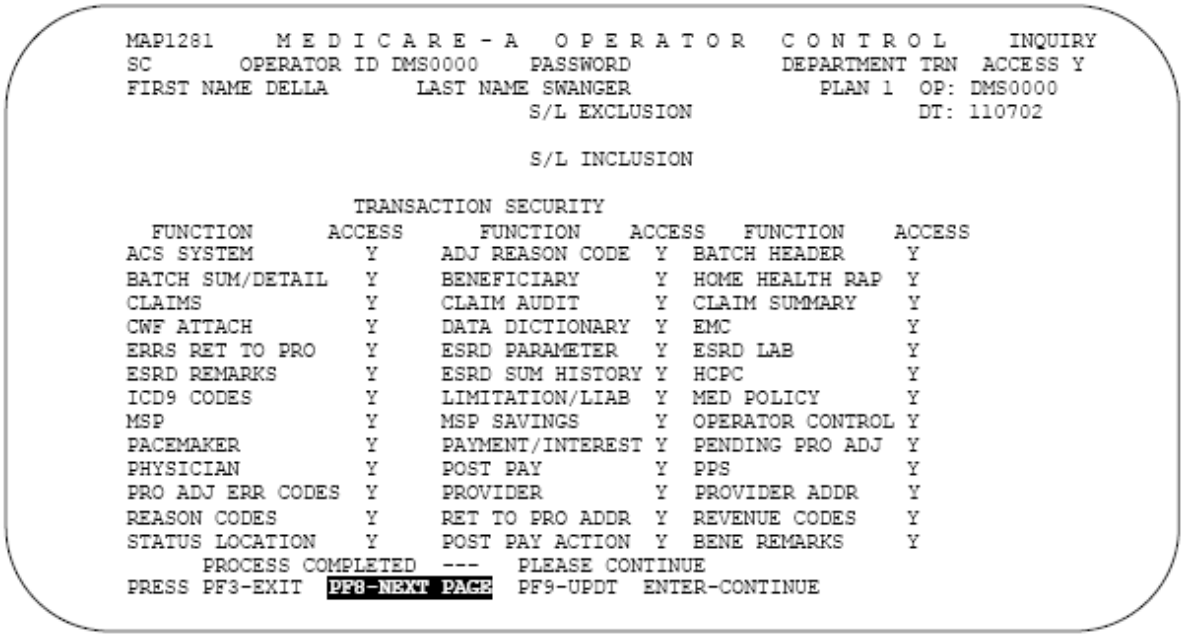
Refer to *CMS Information Security Acceptable Risk Safeguards (ARS) Including CMS Minimum Security Requirements*, Appendix A, *CMS Minimum Security Requirements for High Impact Level Data*, for the applicable CMSRs.

APPENDIX B - GLOSSARY

ARS	Acceptable Risk Safegaurd
CMS	Centers for Medicare & Medicaid Services
CMSR	CMS Minimum Security Requirement
CWF	Common Working File
DDE	Direct Data Entry
DME	Durable Medical Equipment
EDC	Enterprise Data Center
EDS	Electronic Data Systems
FI	Fiscal Intermediary
FISCAM	Federal Information Systems Audit and Control Manual
FISS	Fiscal Intermediary Shared System
FY	Fiscal Year
HIPAA	Health Insurance Portability and Accountability Act
HSPD	Homeland Security Presedential Directive
MAC	Medicare Administrative Contractor
MCS	Multi Carrier System
NIST	National Institute of Standards and Technology
PwC	PricewaterhouseCoopers LLP
SAFE	System Auditing Function Expert
SP	Special Publication
VIPS	ViPS, Inc., formerly Viable Information Processing Systems
VMS	ViPS Medicare System

APPENDIX C - FISS OPERATOR CONTROL FILE EXAMPLE[2]

Figure 1 Screen 1



```
MAP1281     M E D I C A R E - A   O P E R A T O R   C O N T R O L     INQUIRY
SC       OPERATOR ID DMS0000    PASSWORD           DEPARTMENT TRN  ACCESS Y
FIRST NAME DELLA       LAST NAME SWANGER              PLAN 1  OP: DMS0000
                                 S/L EXCLUSION                  DT: 110702

                                 S/L INCLUSION

                    TRANSACTION SECURITY
  FUNCTION      ACCESS      FUNCTION    ACCESS   FUNCTION    ACCESS
ACS SYSTEM         Y     ADJ REASON CODE  Y  BATCH HEADER     Y
BATCH SUM/DETAIL   Y     BENEFICIARY      Y  HOME HEALTH RAP  Y
CLAIMS             Y     CLAIM AUDIT      Y  CLAIM SUMMARY    Y
CWF ATTACH         Y     DATA DICTIONARY  Y  EMC              Y
ERRS RET TO PRO    Y     ESRD PARAMETER   Y  ESRD LAB         Y
ESRD REMARKS       Y     ESRD SUM HISTORY Y  HCPC             Y
ICD9 CODES         Y     LIMITATION/LIAB  Y  MED POLICY       Y
MSP                Y     MSP SAVINGS      Y  OPERATOR CONTROL Y
PACEMAKER          Y     PAYMENT/INTEREST Y  PENDING PRO ADJ  Y
PHYSICIAN          Y     POST PAY         Y  PPS              Y
PRO ADJ ERR CODES  Y     PROVIDER         Y  PROVIDER ADDR    Y
REASON CODES       Y     RET TO PRO ADDR  Y  REVENUE CODES    Y
STATUS LOCATION    Y     POST PAY ACTION  Y  BENE REMARKS     Y
     PROCESS COMPLETED   ---   PLEASE CONTINUE
PRESS PF3-EXIT  PF8-NEXT PAGE  PF9-UPDT  ENTER-CONTINUE
```

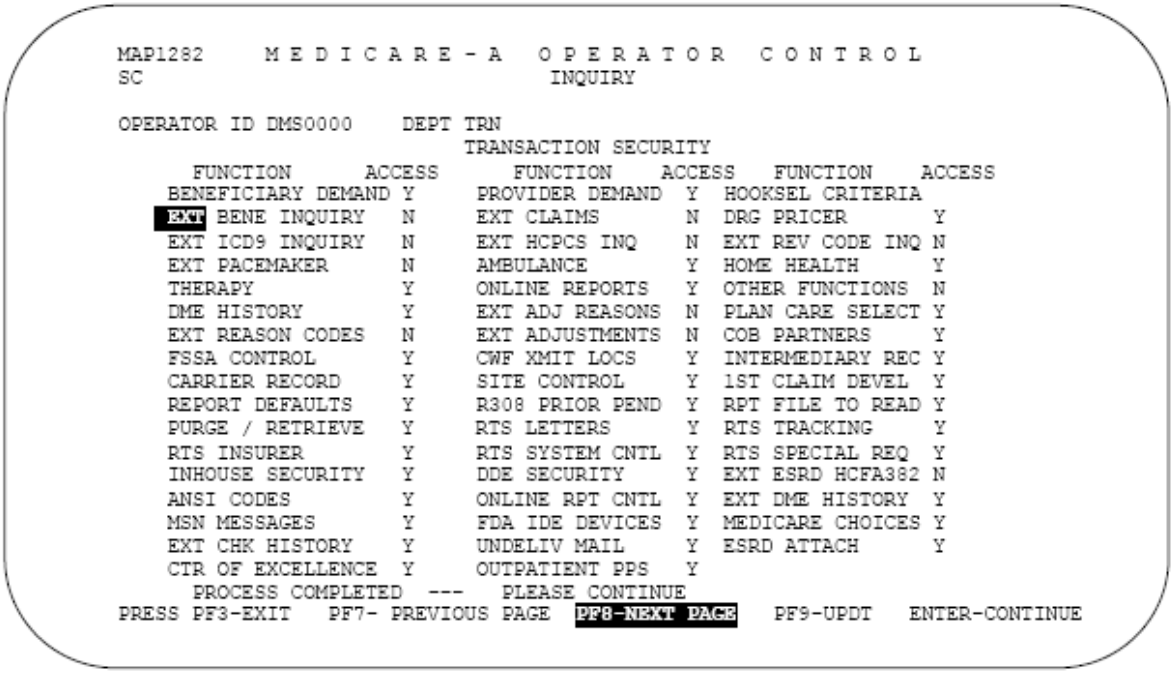
Table 1 Screen 1 Field Descriptions

Field Name	Description
OPERATOR ID	Operator ID - 9 digit alphanumeric field - Enter the Operator ID number. The customer may assign any series of numbers or alphanumeric characters for the employee identification number. The first six positions may be the Provider number. The last three positions may be left blank or assigned a unique value to identify a chain provider or some other sub-classification for clarification
PASSWORD	Password – 9-digit alphanumeric field; the password is used in conjunction with the Operator ID for accessing FISS files. The entered password cannot be viewed on the screen. When changing the password, it is suggested that the field be cleared by using <END> before typing the new password in case there are differences in length between the new and old password.
DEPARTMENT	Department - 3 digit alphanumeric field - Enter the department name or number in the Department field. The entry in this field may be either an abbreviation of the employee's department name or the employee's cost center number. For external or Direct Data Entry providers, 'EXT' must be entered in this field.

[2] Information was obtained from the Arkansas Blue Cross Blue Shield Introduction to FISS Training Participant Guide, version 6/14/2005.

Field Name	Description
ACCESS	Access - 1 digit alphanumeric field - The Access field in the upper right hand corner of the screen is for use with external or Direct Data Entry provider's security for accessing multiple provider number claims information. Valid Values: N - No, the provider cannot access claim information for multiple provider numbers via the Alias ID assignment on Screen 2. A - Yes, the provider can access claim information for multiple provider numbers as indicated in the alias identification assignment section on Screen 2. Y - Y, THIS VALUE SHOULD BE USED ONLY BY THE INTERMEDIARY CUSTOMER SERVICE AND TRAINING DEPARTMENT. This value allows access to all providers. The system will default to 'N' by skipping the access field.
DEPARTMENT	Department – 3-digit alphanumeric field - Enter the department name or number in the Department field. The entry in this field may be either an abbreviation of the employee's department name or the employee's cost center number. For external or Direct Data Entry providers, 'EXT' must be entered in this field.
FIRST NAME	First Name – 10-digit alphanumeric field - Enter the first name of the employee.
LAST NAME	Last Name – 20-digit alphanumeric field - Enter the last name of the employee.
S/L INCLUSION	S/L Inclusion - 6 digit alphanumeric field - Enter up to ten status and location values (ten additional available on Page 3 for total of twenty) field to accommodate an employee performing certain functions. The first position represents the status. The following five positions represent location. The layout of the ten positions in this field is: X xxxxx X xxxxx, etc. EXAMPLE 1: If a claims entry employee is only permitted to work consistency and administrative edits for claims entry, this can be controlled by listing the Consistency Edit Driver and the Administrative Edit Driver as inclusions on the employee's Operator Control File, i.e., 'S' 'M0501', 'S' 'M0601', 'S' 'M1501'. By doing this, the employee will be able to enter claims and work suspended claims with consistency and administrative errors only. This employee could not access claims with duplicate errors, entitlement errors, etc. An error message would occur if the employee tried to work a claim with these types of errors. If the Intermediary wants DDE claims to move to SB9000 in lieu of stopping at SB2500, the Systems Control File flag must be set to 'Y' and it is suggestedthe following Status/Location be added to the Operator Control File S/L INCLUSION field: SB0100, SM04XX, SM05XX, SM06XX, SM15XX and TB99XX.
TRANSACTION SECURITY ACCESS:	Transaction Security Access - The access field identifies the type of transaction security. Valid Values: Y - Employee can enter, update or inquire I - Employee can only inquire N - Employee cannot access the function. The system will default to an 'N' if the field is left blank. Enter one of the above values in the access field of each function or skip the field so the system will default to an 'N'. The cursor will move to the next field either by an entry in a field or by the<TAB>/skip key being depressed. When entering a new operator, it is suggested that you hold the 'Y' or 'I' down to fill all access fields then go back and restrict those areas the operator will not be allowed to access. FOR DDE PROVIDERS ALL TRANSACTION SECURITY FUNCTION ACCESSES ON MAP1281 ARE 'N'.

Figure 2 Screen 2



```
MAP1282     M E D I C A R E - A   O P E R A T O R   C O N T R O L
SC                                INQUIRY

OPERATOR ID DMS0000    DEPT TRN
                          TRANSACTION SECURITY
      FUNCTION      ACCESS      FUNCTION    ACCESS   FUNCTION    ACCESS
    BENEFICIARY DEMAND Y     PROVIDER DEMAND  Y  HOOKSEL CRITERIA
    EXT BENE INQUIRY   N     EXT CLAIMS       N  DRG PRICER       Y
    EXT ICD9 INQUIRY   N     EXT HCPCS INQ    N  EXT REV CODE INQ N
    EXT PACEMAKER      N     AMBULANCE        Y  HOME HEALTH      Y
    THERAPY            Y     ONLINE REPORTS   Y  OTHER FUNCTIONS  N
    DME HISTORY        Y     EXT ADJ REASONS  N  PLAN CARE SELECT Y
    EXT REASON CODES   N     EXT ADJUSTMENTS  N  COB PARTNERS     Y
    FSSA CONTROL       Y     CWF XMIT LOCS    Y  INTERMEDIARY REC Y
    CARRIER RECORD     Y     SITE CONTROL     Y  1ST CLAIM DEVEL  Y
    REPORT DEFAULTS    Y     R308 PRIOR PEND  Y  RPT FILE TO READ Y
    PURGE / RETRIEVE   Y     RTS LETTERS      Y  RTS TRACKING     Y
    RTS INSURER        Y     RTS SYSTEM CNTL  Y  RTS SPECIAL REQ  Y
    INHOUSE SECURITY   Y     DDE SECURITY     Y  EXT ESRD HCFA382 N
    ANSI CODES         Y     ONLINE RPT CNTL  Y  EXT DME HISTORY  Y
    MSN MESSAGES       Y     FDA IDE DEVICES  Y  MEDICARE CHOICES Y
    EXT CHK HISTORY    Y     UNDELIV MAIL     Y  ESRD ATTACH      Y
    CTR OF EXCELLENCE  Y     OUTPATIENT PPS   Y
      PROCESS COMPLETED  ---   PLEASE CONTINUE
PRESS PF3-EXIT   PF7- PREVIOUS PAGE  PF8-NEXT PAGE   PF9-UPDT   ENTER-CONTINUE
```

Table 2 Screen 2 Field Descriptions

Field Name	Description
OPERATOR ID	Operator ID – Systematically carried forward from page one.
DEPARTMENT	Department Name – Systematically carried forward from page one.
BENEFICIARY DEMAND	Beneficiary Demand – This field provides access capability/security to the HIGLAS beneficiary on-demand screen.
EXT BENE INQUIRY	External Beneficiary Inquiry - An external or DDE provider uses the External Beneficiary Inquiry to research beneficiary information.
EXT ICD9 INQUIRY	External International Classification of Diseases - 9th Revision - Clinical Modification Inquiry - The external ICD- 9-CM file provides an inquiry method for external or DDE providers on valid ICD-9-CM coding. This file contains all ICD-9-CMS not just those specific to Medicare.
EXT PACEMAKER	External Pacemaker - The external Pacemaker file (attachment) provides a mechanism for DDE providers to enter pacemaker data with their initial submission of the claim. This attachment is no longer required.
THERAPY	Therapy - The Therapy file (attachment) provides a mechanism for the DDE provider to enter therapy information with their initial submission of the claim as well as a mechanism for internal (Intermediary) entry of therapy information with the initial claim. The Therapy file has a unique screen per therapy discipline, e.g., Physical Therapy, Speech Therapy, etc.; it is accessed through the Claim File on Page 4 for DDE and Page 7 of the claim record for internal entry.
DME HISTORY	Durable Medical Equipment History - The DME History file (attachment) provides a mechanism for the DDE provider to enter DME history information with their initial submission of the claim as well as a mechanism for internal (Intermediary) entry of DME history information with the initial claim.

Field Name	Description
EXT REASON CODES	External Reason Codes - The external Reason Codes file provides an inquiry method for DDE providers for the definitions of the five-position reason code that appears on the claim record and various reports.
FSSA CONTROL	FSSA Control - This field identifies the FSSA control file.
CARRIER RECORD	Carrier Record - The Carrier Record file provides an on-line file for carrier number, name, address, telephone number, etc. Items from this file are used on various FISS reports.
REPORT DEFAULTS	Report Defaults - Not operative; this field is for future use
PURGE/RETRIEVE	Purge/Retrieve Parameter File - This file allows each customer site to control the purging and/or retrieval of FISS files and the duration a record should be retained on such files.
RTS INSURER	Recovery and Tracking System Insurer - The Insurer Detail file allows the Operator to view or modify information in the RTS system for each insurer record created.
INHOUSE SECURITY	In-house Security - This field indicates what type of authority a given Intermediary operator (Inquiry only or update) has to the In-house Security screen.
ANSI CODES	ANSI Reason Code File - Will allow the operator to access the ANSI reason code file based on the code entered in the access field.
MSN MESSAGES	Medicare Secondary Notice Massages - This field defines the access authority for the MSN Messages in the ACS System.
EXT CHK HISTORY	External Check History - This field allows the Intermediary operator to grant access to the Check History Screen (MAP1B01).
CTR OF EXCELLENCE	Centers of Excellence - This field allows the operator to update the Centers of Excellence DRG rates file.
PROVIDER DEMAND	Provider Demand – This field provides access capability/security to the HIGLAS provider on-demand screen.
EXT CLAIMS	External Claims - A DDE provider uses the external Claims file to enter, correct and research claims. This field is for DDE providers only.
EXT HCPCS INQ	External Healthcare Common Procedure Coding System Inquiry - The external HCPCS file provides an inquiry method for DDE providers on the use of HCPCS coding.
AMBULANCE	Ambulance - The Ambulance file (attachment) provides a mechanism for the DDE provider to enter ambulance information with their initial submission of the claim as well as a mechanism for the internal (Intermediary) entry of ambulance information with the initial claim.
ONLINE REPORTS	On-Line Reports - The On-Line Reports file provides a mechanism for the DDE provider to view various on-line reports.
EXT ADJ REASONS	External Adjustment Reasons - The external Adjustment Reason file provides an inquiry method for DDE providers to access the definition of the two-position adjustment reason code that appears on the claim record and various reports.
EXT ADJUSTMENTS	External Adjustments - This field indicates whether or not a DDE provider has the authority to enter adjustment claims.
CWF XMIT LOCS	Common Working File Transmit Locations - The CWF Transmit Location file provides a customer-controlled screen to identify claim locations to be transmitted to CWF.
SITE CONTROL	Site Control - This field indicates whether the operator has access to the Site Control file.
R308 PRIOR PEND	R308 Prior Pending - Not operative; this field is for future use.

Field Name	Description
RTS LETTERS	Recovery and Tracking System Letters - The Demand Letter file allows each plan to house letters to be sent in the Demand Package.
RTS SYSTEM CNTL	Recovery and Tracking System Control - The System Control File Maintenance file is used to initiate each recovery process.
DDE SECURITY	Direct Data Entry Security - This field indicates what type of authority a given Intermediary operator has to the DDE Security screen.
ONLINE RPT CNTL	On-Line Report Control - This field indicates what type of authority the Intermediary operator has to the On-Line Report Screen.
FDA IDE DEVICES	Federal Drug Administration Investigational Device Exemption - This field defines the access authority for file FSSIDEB which contains a list of valid IDE codes and the providers that are authorized to use them.
UNDELIV MAIL	Undeliverable Mail - This field indicates whether or not the operator has inquiry or update access to the Undeliverable Mail screen.
OUTPATIENT PPS	Outpatient Provider Specific - This field defines whether the provider has access to the Outpatient Provider Specific file to make inquiries, updates, and create new entries for providers that are subject to OPPS.
HOOKSEL CRITERIA	Hook Selection Criteria – This field provides access to the Hook Selection (MAP1A71, MAP1A72, MAP1A73, MAP1A74, and MAP1A75) to make entries, updates, or inquires.
DRG PRICER	Diagnosis Related Group Pricer - The DRG Pricer file contains the Grouper and Pricer software programs for determining the reimbursement and diagnosis related grouping of a Medicare inpatient claim.
EXT REV CODE INQ	External Revenue Code Inquiry - The external Revenue Code file provides an inquiry method for external or DDE providers on the appropriate use of Revenue Codes within the Fiscal Intermediary Standard System.
HOME HEALTH	Home Health - The Home Health file provides a mechanism for the DDE provider to enter home health information (attachment) their initial submission of the claim as well as a mechanism for internal (Intermediary) entry of home health information with the initial claim.
OTHER FUNCTIONS	Other Functions - The Other Functions file was developed by the DDE Workgroup for future functions and is currently not operative.
PLAN CARE SELECT	Plan of Care Select - The Plan of Care Select file is a selection screen for the home health plan of care per beneficiary for DDE providers.
COB PARTNERS	Coordination of Benefits Trading Partners - This field indicates whether or not the operator has inquiry or update access to the COB Trading Partners screen.
INTERMEDIARY REC	Intermediary Record - The Intermediary Record file provides an on-line file for Intermediary number, name, address, telephone, etc. Items from this file are used on various FISS reports.
1ST CLAIM DEVEL	First Claim Development - This field is used to indicate whether or not the operator has inquiry, entry or update access to the First Claim Development screen.
RPT FILE TO READ	Report File to Read - Not operative; this field is for future use.
RTS TRACKING	Recovery and Tracking System Tracking - The Tracking Detail file allows the operator to view or modify information contained in the RTS system for each Report ID (HIC and DCN).
RTS SPECIAL REQ	Recovery and Tracking System Special Requests - The Special Request file allows for holding and releasing of tracking records. It also can be used for insurer name and/or address changes.
EXT ESRD HCFA382	External ESRD HCFA382 - The field defines whether the DDE provider has access authority for the DDE HCFA-382 screen.

Field Name	Description
EXT DME HISTORY	External DME History - This field defines whether the DDE provider has access authority for the DME History file.
MEDICARE CHOICES	Medicare Choices - This field defines the access authority for Medicare Choices.
ESRD ATTACH	ESRD Attachment - The ESRD Attachment file allows the DDE provider to enter ESRD attachment information with their initial submission of the claim and allows the internal (Intermediary) operator to enter ESRD attachment with the initial claim.

Figure 3 Screen 3

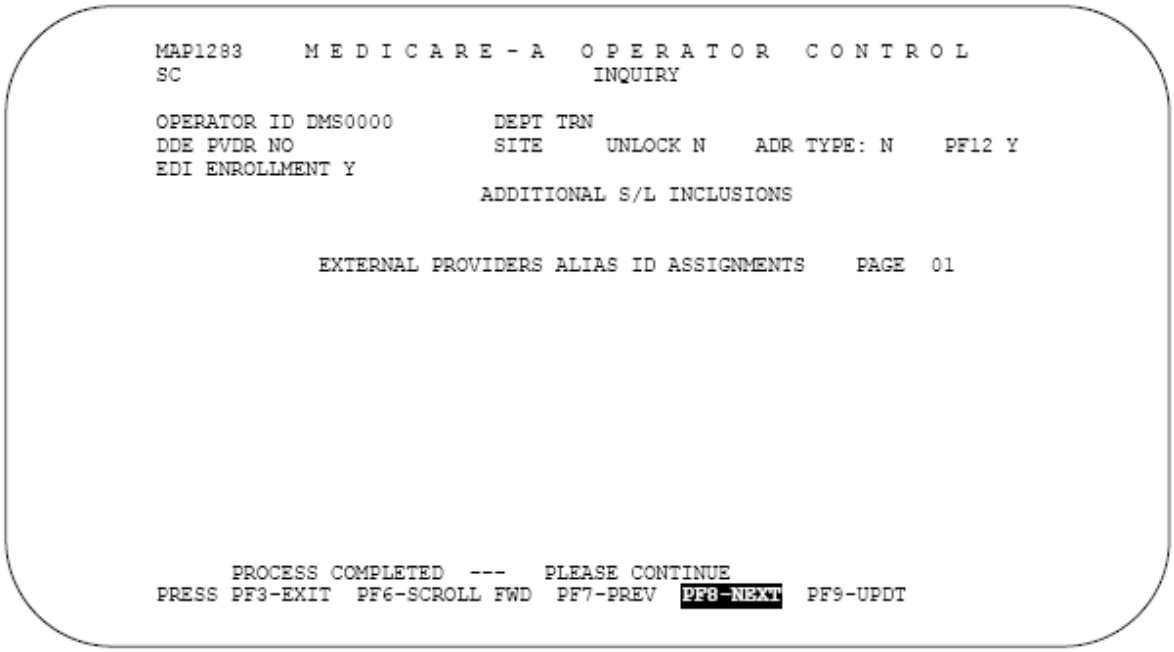


Table 3 Screen 3 Field Descriptions

Field Name	Description
OPERATOR ID	Operator ID – Systematically filled from Page one.
DEPT	Department Name – Systematically filled from Page one.
DDE PVDR NO	DDE Provider Number – 9-digit alphanumeric field - Enter the provider number associated with the Operator ID. The provider entered here must be a valid provider on the Provider File. In addition, this field is used for external operators that are directly associated with one or more provider(s) 'chain Providers'. The primary provider number entered in this field is systematically filled on various DDE screens.

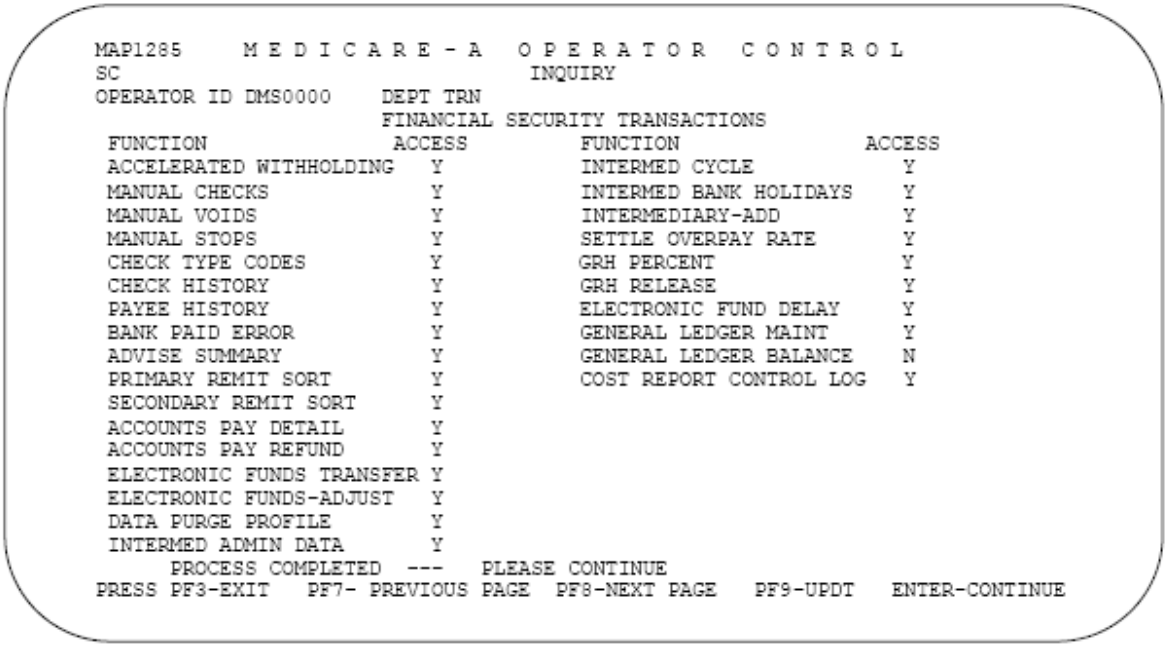
Field Name	Description
SITE	Site – 2-digit numeric field identifies the customer assigned site identification used to restrict access to inquiry, entry and update of claims when the same Intermediary utilizes multiple claim processing sites. When this field is entered, the site indicator of the operator is verified against the site indicator of the provider file to determine if claims can be inquired upon, entered, or updated for the provider in question. This is an optional customer-defined field used only by Intermediaries with multiple processing sites, i.e., Western Penn.
UNLOCK	Unlock – 1-digit alphanumeric field - This field identifies whether an operator can process claims containing a provider number associated with a specific site indicator code on the provider file. The field functions as an override code. Valid Values: Y - Yes, override site indicator N - Do not allow override of site indicator Blank - Do no allow override of site indicator
ADR TYPE	ADR Type - This field indicates to the system whether the operator is authorized to view Additional Development Requests via DDE. Valid Values: Y - Yes, this operator is authorized to view ADRs online. N - No, this operator is not authorized to view ADRs on-line, it is expected that hard-copy ADRs will be generated. B - Yes, this operator is authorized to view ADRs online, it is also expected that hard copy. Blank - Defaults to 'N'. No, this operator is not authorized to view ADRs on-line, it is expected that ADRs will be generated hard copy. If the Intermediary is not careful in coordinating the updating of the Provider File 'DDE ADR TYPE' field with the updating of the Operator Control File 'ADR TYPE' field, it is possible to prevent the provider from receiving ANY ADRs, at all. This could occur if the provider file is updated to reflect that a provider should only receive on-line ADRs when the provider does not have DDE capability (or has no operator authorized to view the ADRs on-line).
PF12	PF12 - This field allows you to use <F12> as a delete function within the core system. Valid Values: Y - The system deletes the file and reports it on the audit report. Blank - The system does not delete the file and does not report it on the audit report. The system recognizes <F12> as an entry key and takes no action.
EDI ENROLLMENT	EDI Enrollment - This field identifies the type of authority the operator has for the EDI Enrollment Form field in the Provider File. Valid Values: Y - Operator authorized to update the EDI Enrollment Form field. N - Operator not authorized to update the EDI Enrollment Form field.
ADDITIONAL S/L INCLUSIONS	Additional S/L Inclusions - This field provides an area to list ten additional status and locations that a particular employee is allowed to work or is included to work, allowing a total of twenty different included status and locations. If the Intermediary wants DDE claims to move to SB9000 in lieu of stopping at SB2500, the Systems Control File flag must be set to 'Y'; in this case, it is suggested the following Status/Location be added to the Operator Control File S/L INCLUSION field: SB0100, SM04XX, SM05XX, SM06XX, SM15XX and TB99XX.

Field Name	Description
EXTERNAL PROVIDERS ALIAS ID ASSIGNMENTS	External Providers Alias ID Assignments – 9-digit alphanumeric field - The purpose of this section of the Operator Control File is to provide security for providers with multiple provider numbers. Enter the additional Medicare provider numbers in this section that a particular provider is authorized to view for claim or reimbursement information, i.e., Hospital 'X' also owns a Home Health Agency (Provider 'A') and a Skilled Nursing Facility (Provider 'B'). The main Operator ID number would be 'X' and alias ID on Screen 3 of the Operator control File would be 'A' and 'B'. This would allow Provider 'X' to view not only claim information from this facility, but also the claim information for Providers 'A' and 'B'. There are three pages with fifty occurrences per page of possible aliases.

Figure 4 Screen 4

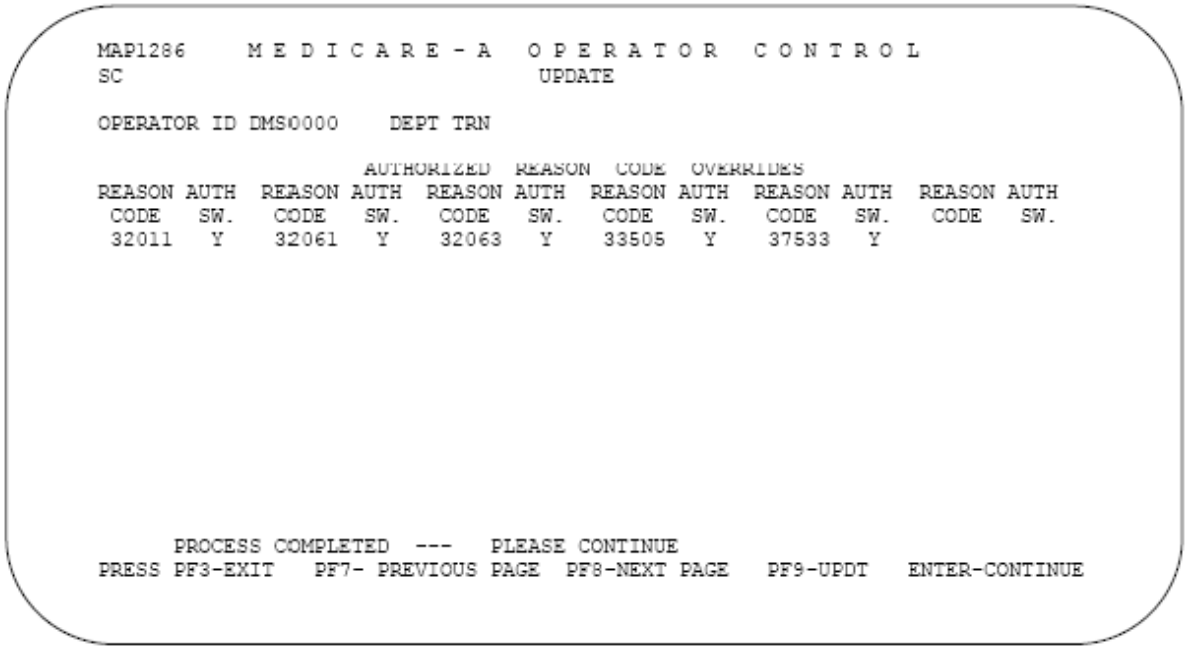
```
MAP1284     M E D I C A R E - A   O P E R A T O R   C O N T R O L
SC                                INQUIRY
OPERATOR ID DMS0000    DEPT TRN
                       FINANCIAL SECURITY TRANSACTIONS
 FUNCTION               ACCESS          FUNCTION               ACCESS
 FINANCIAL-MASTER      (M)  Y           CASH DISBURSEMENTS        Y
 OTHER PAY             (M)  Y           HCFA 456                  Y
 BENE RECONCILIATION   (M)  Y           HCFA 1521                 Y
 PAYMENT               (M)  Y           HCFA 1522                 Y
 SETTLEMENT            (M)  Y           HCFA IBPR REPORT          Y
 WITHHOLDINGS          (M)  Y           PENALTY RELEASE           Y
 MANUAL CHECK PROCESS  (M)  Y           REFUND                    Y
 CHECKS                (M)  Y           ACCELERATED PAYMENT       Y
 REMITTANCE            (M)  Y           SETTLEMENT (ADD)          Y
 ACCOUNTS PAYABLE      (M)  Y           SETTLEMENT CASH RECOUP    Y
 ELECTRONIC FUNDS      (M)  Y           SETTLEMENT ACCOUNTS REC   Y
 SYSTEM PROFILE        (M)  Y           SETTLEMENT ADJUSTMENTS    Y
 INTERMEDIARY ADMIN    (M)  Y           PROVIDER STATEMENTS       Y
 SYSTEM ADMIN          (M)  Y           SETTLEMENT INQUIRY        I
 CHART OF ACCOUNTS          Y           PENALTY                   Y
 CASH RECEIPTS              Y           CLAIM ACCOUNTS REC        Y
 BENE RECONCILIATION        Y           SETTLEMENT                Y
      PROCESS COMPLETED  ---   PLEASE CONTINUE
PRESS PF3-EXIT   PF7- PREVIOUS PAGE  PF8-NEXT PAGE   PF9-UPDT   ENTER-CONTINUE
```

Figure 5 Screen 5



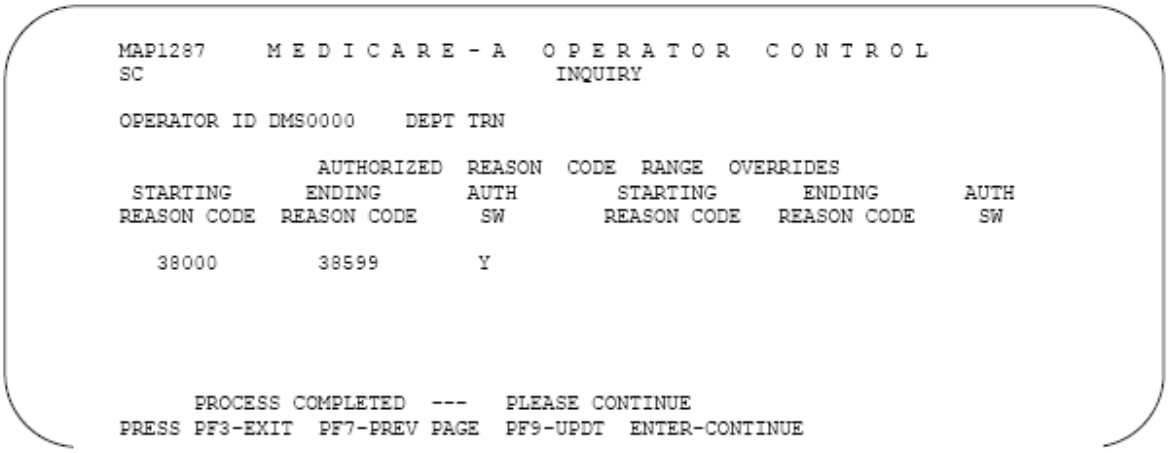
```
MAP1285     M E D I C A R E - A   O P E R A T O R   C O N T R O L
SC                                INQUIRY
OPERATOR ID DMS0000    DEPT TRN
                       FINANCIAL SECURITY TRANSACTIONS
 FUNCTION               ACCESS          FUNCTION               ACCESS
 ACCELERATED WITHHOLDING   Y            INTERMED CYCLE            Y
 MANUAL CHECKS             Y            INTERMED BANK HOLIDAYS    Y
 MANUAL VOIDS              Y            INTERMEDIARY-ADD          Y
 MANUAL STOPS              Y            SETTLE OVERPAY RATE       Y
 CHECK TYPE CODES          Y            GRH PERCENT               Y
 CHECK HISTORY             Y            GRH RELEASE               Y
 PAYEE HISTORY             Y            ELECTRONIC FUND DELAY     Y
 BANK PAID ERROR           Y            GENERAL LEDGER MAINT      Y
 ADVISE SUMMARY            Y            GENERAL LEDGER BALANCE    N
 PRIMARY REMIT SORT        Y            COST REPORT CONTROL LOG   Y
 SECONDARY REMIT SORT      Y
 ACCOUNTS PAY DETAIL       Y
 ACCOUNTS PAY REFUND       Y
 ELECTRONIC FUNDS TRANSFER Y
 ELECTRONIC FUNDS-ADJUST   Y
 DATA PURGE PROFILE        Y
 INTERMED ADMIN DATA       Y
      PROCESS COMPLETED  ---   PLEASE CONTINUE
PRESS PF3-EXIT   PF7- PREVIOUS PAGE  PF8-NEXT PAGE   PF9-UPDT   ENTER-CONTINUE
```

Figure 6 Screen 6



```
MAP1286     M E D I C A R E - A   O P E R A T O R   C O N T R O L
SC                                UPDATE

OPERATOR ID DMS0000    DEPT TRN

                     AUTHORIZED  REASON  CODE  OVERRIDES
REASON AUTH  REASON AUTH  REASON AUTH  REASON AUTH  REASON AUTH  REASON AUTH
 CODE   SW.   CODE   SW.   CODE   SW.   CODE   SW.   CODE   SW.   CODE   SW.
 32011   Y    32061   Y    32063   Y    33505   Y    37533   Y




      PROCESS COMPLETED  ---   PLEASE CONTINUE
PRESS PF3-EXIT   PF7- PREVIOUS PAGE  PF8-NEXT PAGE   PF9-UPDT   ENTER-CONTINUE
```

Figure 7 Screen 7



```
MAP1287     M E D I C A R E - A   O P E R A T O R   C O N T R O L
SC                                INQUIRY

OPERATOR ID DMS0000    DEPT TRN

                AUTHORIZED  REASON  CODE  RANGE  OVERRIDES
 STARTING       ENDING       AUTH         STARTING       ENDING       AUTH
REASON CODE  REASON CODE      SW         REASON CODE   REASON CODE     SW

   38000         38599         Y




      PROCESS COMPLETED  ---   PLEASE CONTINUE
PRESS PF3-EXIT  PF7-PREV PAGE  PF9-UPDT  ENTER-CONTINUE
```

APPENDIX D - MCS Clerk Record Update Screen[3] Example

Figure 8 Screen 1

```
TASK 1...                  CLERK RECORD UPDATE
KEY 2.............                                              3...........

ACTION CODE  4           A = ADD     CLERK RECORD               PF3=MENU
                         C = CHANGE  CLERK RECORD               PF8=PAGE2
                         D = DELETE  CLERK RECORD
                         I = INQUIRY CLERK RECORD

CLERK   5...             NEXT CLERK  6...

NAME  FIRST              LAST              DEPT DIV  UNIT   LAST UPDATED   BY
      7...........       8.............    9..   10   11      12......   .13.

      NICKNAME           B-DATE     HOLD    STATE INDICATORS
      14........          15..       16     17 18 .. . .. . .. .



    ONLINE SCREEN ACCESS                FILE MAINTENANCE AUTHORIZATION


AGE      19      ACIS 1   36         ADS              50    MM              65
AUDIT    20      ACIS 2   37         CENSUS UPDATES   51    NU              66
CLERK    21      ACIS 3   38         CRITERIA         52    SU              67
DEOL     22      ACIS 4   39         CWF ERROR        53    CO              68
GT       23      ACIS 5   40         DIAGNOSIS        54
HELP     24      ACIS 6   41         EDIT             55    2590 REPORT
IS       25      E1       42         EDIT/AUDIT       56    AUTHORIZATION   69
LCEF     26      E2       43         EOMB             57
MSG      27      E3       44         HARDCODED E/A    58
MSPR     28      C1       45         MODIFIER         59    PSUP            70
SMRT     29      C2       46         NARRATIVE        60
SS       30      C3       47         PCF              61    SAFE
TRNG     31      C4       48         PROCEDURE        62    S1  71
CLRK CA  32      HR       49         TACS             63    S2  72
VH       33                          SCF              64    S3  73
LC       34
HIMR SS  35



MSG 74.............................................
```

Table 4 Screen 1 Field Descriptions

No.	Field Name	Business Name/Description
1	TASK	This field may be utilized to input a next transaction code for movement from CLRK screen.

[3] Information was obtained from the Electronic Data Systems System Security and Operator Authorization Manual, Clerk Record Update Screen Specifications, version 2/16/06.

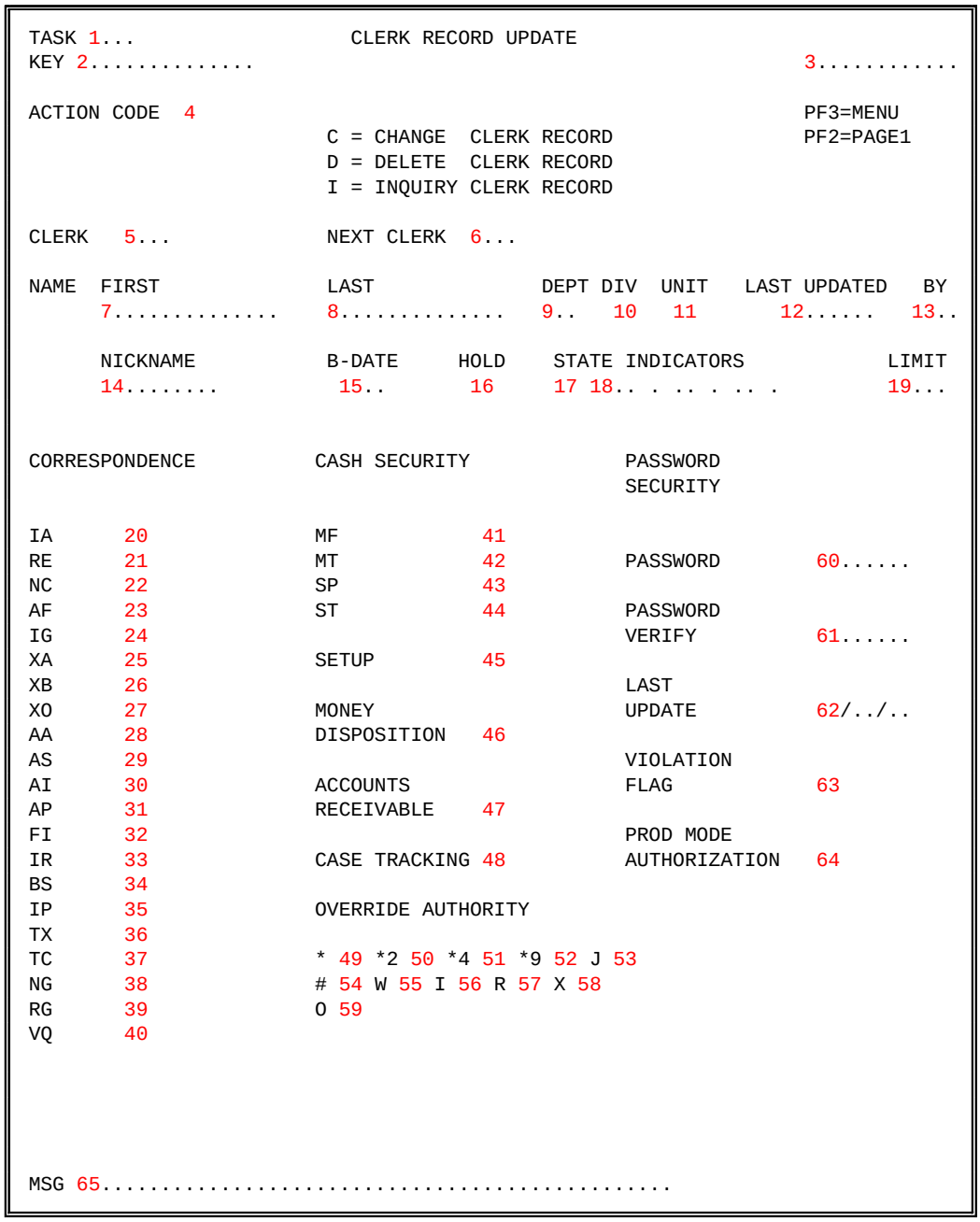
No.	Field Name	Business Name/Description
2	KEY	This field may be utilized to input a parameter or key for the next transaction selection. This is used in conjunction with the TASK field. Task Key CLRK Clerk number AUDT None SS Department, division and unit code IS Clerk number
3	UNTAGGED	Current date – Gregorian format: Month Alpha Day Numeric 2 Year Numeric 4
4	ACTION CODE	Enter the desired action code. Valid values: A Add a record D Delete a record C Change a record I Inquire Note: An inquiry transaction must be performed prior to a delete or change transaction.
5	CLERK	Enter the desired clerk ID.
6	NEXT CLERK	Enter the next clerk ID, used for continuous transactions.
7	FIRST	Clerk's first name.
8	LAST	Clerk's last name.
9	DEPT	Department number of clerk.
10	DIV	Division number.
11	UNIT	Unit number.
12	LAST UPDATED	The most recent date the Clerk Record Update screen undergoes an add/change transaction. NOTE: The deleted records will not display online. The Clerk Record Report will list deletes.
13	BY	Clerk ID of the person last performing an update to the Clerk Record Update screen.
14	NICKNAME	Nickname of the individual assigned to the Clerk ID on display, may be spaces.
15	B-DATE	Date of birth. Format: MMDD
16	HOLD	Supervisor tool for review of claims processed by a specific clerk ID. If left blank, this field defaults to a value of N.

No.	Field Name	Business Name/Description
17	STATE INDICATORS	Identifies up to 4 states the clerk ID is authorized to key data into. State indicators vary by carrier. The State Codes Clerk State1-4 fields on the Online Plan Code SPITAB table is maintained by EDS. Reference specification S1326000. For example, for: Massachusetts MA ME NH VT Texas TX RH BO DN Illinois IL Ohio OH/WV. The State Codes Clerk State 1-4 fields on the Online Plan Code SPITAB table are maintained by EDS. A carrier may specify up to four two-digit 'state' indicators to display on the on-line clerk screen. The number of indicators must correspond to the number of 'states' being used by the carrier. For example, if a single state carrier uses MCS state 1 ICN regions, one two-digit state indicator would be displayed on the clerk screen to allow examiners to be authorized to enter claims/correspondence for that state.
18	STATE INDICATORS	This field identifies state(s) in which the clerk is authorized to process. Authorization value is X. Unauthorized value is blank.
19	AGE	Authorization to inquire the AGED CLaims - Selection (AGE) Screen. Valid values are N and I.
20	AUDIT	Authorization to access the Audit (AUDT) Screen. Valid values are N, I, and U
21	CLERK	Authorization to access the Clerk (CLRK) Screen. Valid values are N, I, and U.
22	DEOL	Authorization to access theData Entry On-Line (deol) Screen for free-format maintenance transactions. Valid values are N and U.
23	GT	Authorization to access the formatted Location Transfer (GT) Screen for general transfers. Valid values are N and U.
24	HELP	Authorization to update the Help Code Lookup(HE) Screen. Valid values are N, I and U.
25	IS	Authorization to access the Individual Statistics (IS) Screen. Valid values are N I and U. N = No access to the the Individual Statistics (IS) Screen I = Access to view only their own Individual Statistics (IS) Screen U = Access to view other clerk id's Individual Statistics (IS) Screen
26	LCEF	Authorization to access Limiting Charge Exception File Inquiry (LCEF) Screens. Valid values are N, I and U.
27	MSG	Authorization to update the Batch Message Update (MSG) Screen. Valid values are N, I and U.
28	MSPR	Authorization to access the MSP Response Entry (MSPR) Screen. Valid values are N and U.
29	SMRT	Authorization to access the Smart (SMRT) Screens. Valid values are N, I and U.
30	SS	Authorization to access the Summary Statistics (SS) Screen. Valid values are N and I
31	TRNG	Authorization to access the Claims/Corr Training Menu (TRNG) Screen. Valid values are N, I, and U.
32	CLRK CA	Authorization to access the Clerk Audit Trail (CA) Screen. The default value is N and all new clerk adds will default to N in the setup.

No.	Field Name	Business Name/Description
33	VH	Authorization to access the MCS PIN Support - History (VH) Screen. Valid values are N and I. The default value is N and all new clerk adds will default to N in the setup.
34	LC	Authorization to access the NCD FILE (LC). Valid values are N and I. At conversion all clerks will be given an I. All new clerks will be given an I in the setup.
35	HIMR SS	Authorization to access the VIPS HIMR Split (HIMR SS) Screen mnemonics. Valid values are N and I. NOTE: Authorization to update eligibility through the SB screen is controlled by the NU flag. Authority to update MSP records through SD is controlled by the SP flag.
36	ACIS 1	Authorization to add, change or delete claim control numbers on the ACIS Menu Screen (ACIS 1). Valid values are N and U.
37	ACIS 2	Authorization to inquire current batches on the Batch Activation Inquiry Screen (ACIS 2). Valid values are N and I.
38	Acis 3	Authorization to inquire single batches on the Batch Activation Single Inquiry Screen (ACIS 3). Valid values are N and I.
39	Acis 4	Authorization to inquire on the Work Scheduler Current Work Groups Screen (ACIS 4). Valid values are N and I.
40	Acis 5	Authorization to Work Scheduler Single Work Groups Screen (ACIS 5). Valid values are N and I.
41	Acis 6	Authorization to access the Reactivate CORR Finalized in Error function, Batch Activation Maintenance Sceen (ACIS 6). Valid values are N and U.
42	E1	Authorization to sign on to an initial batch from the Claims Batch Screen Function (E1). Valid values are N and U.
43	E2	Authorization to sign on to a continued batch from the Claims Batch Screen Function (E2). Valid values are N and U.
44	E3	Authorization to sign on to a non-coord batch from the Claims Batch Screen Function (E3). Valid values are N and U.
45	C1	Authorization to perform an ICN list fetch from the Claims Batch Screen Function (C1). Valid values are N and U.
46	C2	Authorization to a perform a batch fetch from the Claims Batch Screen Function (C2). Valid values are N and U.
47	C3	Authorization to sign on to an ADS batch from the Claims Batch Screen Function (C3). Valid values are N and U.
48	C4	Authorization to perform a work schedule fetch from the Claims Batch Screen Function (C4). Valid values are N and U
49	HR	Authorization to access and perform updates to the HIGLAS Rejected Claims (HR) screen. Valid values are N, I, and U. All carriers will default to N in this field. Only carriers on HIGLAS can update this field with I or U.
50	ADS	Authorization to update the ADS question file from the File Maintenance Menu (FMM) Screen. Valid values are N, I, and U.
51	CENSUS UPDATES	Authorization to maintenance the bene census information on the Beneficiary Eligibility Update 2 (N2) Screen. Valid values are N, I, and U.
52	CRITERIA	Authorization to update the Criteria File from the File Maintenance Menu (FMM) Screen. Valid values are N, I, and U.
53	CWF ERROR	Authorization to update the CWF Error Code File from the File Maintenance Menu (FMM) Screen. Valid values are N, I, and U.
54	DIAGNOSIS	Authorization to update the Diagnosis File from the File Maintenance Menu (FMM) Screen. Valid values are N, I, and U.

No.	Field Name	Business Name/Description
55	EDIT	Authorization to update the online Edit screen from the File Maintenance Menu (FMM) Screen. Valid values are N, I, and U.
56	EDIT/AUDIT	Authorization to update the Edit/Audit File from the File Maintenance Menu (FMM) Screen. Valid values are N, I, and U.
57	EOMB	Authorization to update the EOMB Message File from the File Maintenance Menu (FMM) Screen. Valid values are N, I, and U.
58	HARDCODED E/A	Authorization to update Hardcoded Edits/Audits identified by the value of EDS on the the EOMB Message File from the File Maintenance Menu (FMM) Screen. Valid values are N and Y. (authorization to update SCC for EDS-controlled edits and audits) Note: This field will default to an N on new clerk entry.
59	MODIFIER	Authorization to update the Modifier File from the File Maintenance Menu (FMM) Screen. Valid values are N, I, and U.
60	NARRATIVE	Authorization to update the Narrative File from the File Maintenance Menu (FMM) Screen. Valid values are N, I, and U.
61	PCF	Authorization to update the Provider Control File (PCF) Screen. Additional security is required on the HXXTPSEC SPITAB Table. Valid values are N, I, and U.
62	PROCEDURE	Authorization to update the Procedure Code File from the File Maintenance Menu (FMM) Screen. Valid values are N, I, and U.
63	TACS	Authorization to update the TACS Letter File from the File Maintenance Menu (FMM) Screen. Valid values are N, I, and U.
64	SCF	Authorization to SCF Utility and Maintenance Screens. Valid values are Y and N. Note: This field will default to an N on new clerk entry.
65	MM	Authorization to update the Other Insurers Maintenance (MM) Screen. Valid values are N, I, and U.
66	NU	Authorization to update the Beneficiary Eligibility Update (NU) Screen. Valid values are N, I, and U.
67	SU	Authorization to update the Beneficiary Status Update (SU) Screen. Valid values are N and U.
68	CO	Authorization to update the Comment (CO) Screen. Valid values are N, I, and U.
69	2590 REPORT AUTHORIZATION	Authorization to update the 2590 Tables Via the CX Screens. Valid values are N, I , and U.
70	PSUP	Authorization to update the MCS PIN Support - Menu (PSUP) Screen. Valid values are I, M, N and U. The default value is N and all new clerk adds will default to N in the setup. I Inquiry only M Update, add or delete U Update or add N No inquiry/No update
71	S1	Authorization to access SAFE and update the Operator Note Screen. Valid values are Y and N.
72	S2	Authorization to request reports within SAFE. Valid values are Y and N.
73	S3	Authorization to update the Systest/Production Control Table within SAFE. Valid values are Y and N.
74	MSG	System generated error/informational message.

Figure 9 Screen 2



```
TASK 1...                  CLERK RECORD UPDATE
KEY 2.............                                          3...........

ACTION CODE  4                                              PF3=MENU
                        C = CHANGE  CLERK RECORD            PF2=PAGE1
                        D = DELETE  CLERK RECORD
                        I = INQUIRY CLERK RECORD

CLERK   5...            NEXT CLERK  6...

NAME  FIRST             LAST             DEPT DIV  UNIT   LAST UPDATED   BY
      7.............    8.............   9..   10   11       12......   13..

      NICKNAME          B-DATE     HOLD    STATE INDICATORS            LIMIT
      14........         15..       16     17 18.. . .. . .. .          19...


CORRESPONDENCE          CASH SECURITY            PASSWORD
                                                 SECURITY

IA      20              MF            41
RE      21              MT            42         PASSWORD        60......
NC      22              SP            43
AF      23              ST            44         PASSWORD
IG      24                                       VERIFY          61......
XA      25              SETUP         45
XB      26                                       LAST
XO      27              MONEY                    UPDATE          62/../..
AA      28              DISPOSITION   46
AS      29                                       VIOLATION
AI      30              ACCOUNTS                 FLAG            63
AP      31              RECEIVABLE    47
FI      32                                       PROD MODE
IR      33              CASE TRACKING 48         AUTHORIZATION   64
BS      34
IP      35              OVERRIDE AUTHORITY
TX      36
TC      37              * 49 *2 50 *4 51 *9 52 J 53
NG      38              # 54 W 55 I 56 R 57 X 58
RG      39              O 59
VQ      40




MSG 65.............................................
```

Table 5 Screen 2 Field Descriptions

No.	Field Name	Business Name/Description
1	TASK	This field may be utlized to input a next transaction code for movement from CLRK screen.

No.	Field Name	Business Name/Description
2	KEY	This field may be utlized to input a parameter or key for the next transaction selection. Task Key CLRK Clerk number AUDT None SS Department, division and unit code IS Clerk number
3	UNTAGGED	Current date – Gregorian format: Month Alpha Day Numeric 2 Year Numeric 4
4	ACTION CODE	Enter the desired action code. Valid values: A Add a record D Delete a record C Change a record I Inquire Note: An inquiry transaction must be performed prior to a delete or change transaction.
5	CLERK	Enter the desired Clerk ID.
6	NEXT CLERK	Enter the next Clerk ID, used for continuous transactions.
7	FIRST	Clerk's first name.
8	LAST	Clerk's last name.
9	DEPT	Department number of clerk.
10	DIV	Division number.
11	UNIT	Unit number.
12	LAST UPDATED	The date on which the clerk's record was last updated. Format :MM/DD/YY
13	BY	Clerk ID of the person performing the last update transaction to the clerk's record.
14	NICKNAME	Clerk nickname, may be spaces.
15	B-DATE	Date of birth. Format: MMDD
16	HOLD	Supervisor tool for review of claims processed by a specific clerk ID. If left blank, this field defaults to a value of N.

No.	Field Name	Business Name/Description
17	STATE INDICATORS	Identifies up to 4 states the clerk ID is authorized to key data into. State indicators vary by carrier. The State Codes Clerk State1-4 fields on the Online Plan Code SPITAB table is maintained by EDS. Reference specification S1326000. For example, for: Massachusetts MA ME NH VT Texas TX RH BO DN Illinois IL Ohio OH/WV. The State Codes Clerk State 1-4 fields on the Online Plan Code SPITAB table are maintained by EDS. Reference specification S1326000. A carrier may specify up to four two-digit 'state' indicators to display on the on-line clerk screen. The number of indicators must correspond to the number of 'states' being used by the carrier. For example, if a single state carrier uses MCS state 1 ICN regions, one two-digit state indicator would be displayed on the clerk screen to allow examiners to be authorized to enter claims/correspondence for that state.
18	STATE INDICATORS	This field identifies state(s) in which the clerk is authorized to process. Authorization value is X. Unauthorized value is blank.
19	LIMIT	Limits the number of online Express Adjustments to be allowed for a given Express Adjustment Batch. The system will produce a history selection limit error if more than this number of claims are selected for an Express Adjustment batch. When this selection error is returned, the clerk will need to revise the event selection criteria on the Define Batch Screen. Valid value is whole number between 0-99999. A clerk file edit will fail if this field is '0' and the XA or XB flag is 'Y.'
20	IA	Authorization to access to the Claim/Adjustment (IA) Function from the Claim (CLAM) Screen for an ICN still in history. Valid values are N and U.
21	RE	Authorization to access a re-opening (RE) Function from the Claim (CLAM) Screen. Valid values are N and U.
22	NC	Authorization to access the No-Claim Adjustment (NC) from the Claim (CLAM) ScreenClaim (CLAM) Screen. Valid values are N and U.
23	AF	Authorization to access the Full Claim Adjustment (AF) Function from the Claim (CLAM) Screen. Valid values are N and U.
24	IG	Authorization to override IA Transaction (IG) from the Claim (CLAM) Screen. Valid values are N and U. Please note if IA is set to 'N' the IG transaction will assume the IA authority level of 'N'.
25	XA	Authorization to access the Transaction List Menu on the MCS Express Adjustments Set-up.(XA) Screen. Valid values are Y or N. A clerk screen edit will fail if this flag is changed to 'Y' but the LIMIT field is zero.
26	XB	Authorization to access the Express Adjustment Menu Screen. Valid values are Y or N. An edit will fail if this flag is changed to 'Y' but the LIMIT field is zero.
27	XO	Authorization to perform Express Adjustments on 'Other' (XO)type adjustments. Valid values are Y or N.
28	AA	Authorization to access the Accounts Payable - ICN/CCN (AA) Screen. Valid values are N, I, and U. NOTE: The value of U (Update) is not valid for HIGLAS carriers.
29	AS	Authorization to access the Account Payable - Payee Summary (AS) Screen. Valid values are N and I.
30	AI	Authorization to access the Claim Dollar Audit Criteria (AL) Screen. Valid values are N and I.

No.	Field Name	Business Name/Description
31	AP	Authorization to access the Accounts Receivable Inquiry by Payee (AP) Screen. Valid values are N and I.
32	FI	Authorization to access the Finicial Inquiry For Special Checks (FI) Screen. Valid values are N and I.
33	IR	Authorization to access the Return Check Inquiry (IR) Screen. Valid values are N and I.
34	BS	Authorization to access the Bank Check Status (BS) Screen. Valid values are N and I.
35	IP	Authorization to access the Checks Issued to Payee (IP) Screen. Valid values are N, I, and U.
36	TX	Authorization to access the TACS Letter Entry Function on the TACS Letter (TX) Screen. Valid values are N and U.
37	TC	Authorization to access the [Suspended TACS Letter Corrections Function from the TACS Letter (TC) Screen. Valid values are N and U.
38	NG	Authorization to override the NC Transaction (NG) from the Claim (CLAM) Screen. Valid values are N and U. Please note if NC is set to 'N', the NG transaction will assume the NC authority level of 'N'.
39	RG	Authorization to override the RE Transaction (RG) from the Claim (CLAM) Screen. Valid values are N and U. Please note if RE is set to 'N', the RG transaction will assume the RE authority of 'N'.
40	VQ	Authorization to access the Claim Credited/Void Query from the Void Query Request (VQ) Screen. Valid values are N and U.
41	MF	Authorization to inquire and update the Multi-Entry Financial (MF) Screen. Valid values are N and U.
42	MT	Authorization to inquire and update the Financial Transaction (FT) Screen. Valid values are N and U. NOTE: The value of U (Update) is not valid for HIGLAS carriers.
43	SP	Authorization to inquire and update the Stop-pay transaction from the Financial Transaction (FT) Screen. Valid values are N and U. NOTE: The value of U (Update) is not valid for HIGLAS carriers.
44	ST	Authorization to perform a Stop-pay Correction transaction from the Financial Transaction (FT) Screen. Valid values are N and U. NOTE: The value of U (Update) is not valid for HIGLAS carriers.
45	SETUP	Authorization to inquire and update the Cash Setup)CS) Screen. Valid values are N and U. NOTE: The value of U (Update) is not valid for HIGLAS carriers.
46	MONEY DISPOSITION	Authorization to perform Money Dispursement transactions. Valid values are N and U. NOTE: The value of U (Update) is not valid for HIGLAS carriers.
47	ACCOUNTS RECEIVABLE	Authorization to inquire and update the Accounts Receivable (AR) Screen. Valid values are N and U. NOTE: The value of U (Update) is not valid for HIGLAS carriers.
48	CASE TRACKING	Authorization to access and maintenance the Case Tracking from the Correspondence and Cash Batch Initiation (CORR) Screen. Valid values are N, I and U. NOTE: The value of U (Update) is not valid for HIGLAS carriers.

No.	Field Name	Business Name/Description
49	*	Overrides edits and audits, when keyed in front of the edit or audit number in the override field.
50	*2	Overrides all duplicate detail audits online, when keyed in the first detail override field. The *2 is passed to batch, where it also overrides all detail duplicate audits. The system defaults with a value of Y.
51	*4	Overrides all header audits when keyed in the 'A' portion of the 'AS' field. This only applies to audits set up with a disposition of 'F' or 'S' on the SCC file. The system defaults with a value of Y.
52	*9	Overrides all audits on a claim when keyed in the 'A' portion of the 'AS' field. . The system defaults with a value of Y.
53	J	Used to upcode or downcode a procedure code, when entered in front of the audit number in the detail override field. The audit will be overridden and will not re-fail in batch even though a critical field has been changed on the detail. The system defaults with a value of Y.
54	#	Performs the same action as the *, except that the audit will be overridden even if a critical field on the detail is changed. The system defaults with a value of Y.
55	W	Used to 'undeny' a claim, when keyed in the header AD field. The 'W' action will be propagated to each detail ASYS field real-time. Used to 'undeny' a detail when keyed in the 'A' portion of the 'ASYS' field on the detail line. I is also used to allow clerk security to use a Y in the ADS Action Code. The system defaults with a value of Y.
56	I	Used to upcode or downcode a procedure, when keyed in the first byte of the override field on the detail. The system defaults with a value of Y.
57	R	Used to reduce a detail's payment by 10%, when keyed in the override field. The system defaults with a value of Y.
58	X	Used to remove the 'R' reduction flag on a detail. The system defaults with a value of Y.
59	O	Used to override CWF error situations: CWF override -1 The system defaults with a value of Y.
60	PASSWORD	Password associated with the clerk ID on the Clerk Record Update (CLRK) Screen. (Note: the current password value does not appear.) This field is used to initialize or reset a clerk password to a specific value. When adding a new clerk record, if no value is keyed in this field, the system sets the initial password to the value of START. If a specific value is keyed, that value becomes the initial password. If this field is cleared to reset a clerk password, the system sets the password to the value 'Start' (when the change action code is used). The keyed values must be 4-8 alphanumeric characters with no imbedded spaces.
61	PASSWORD (VERIFY)	This password verification field is used to verify the value in the previous password field. The value must equal the value in the password field. When you clear the Password field you must also clear this field on the Clerk Record Update (CLRK) Screen.

No.	Field Name	Business Name/Description
62	LAST UPDATE	Date of the last password update on the Clerk Record Update (CLRK) Screen. When the password is reset from this screen, the date is always set to 01/01/65 to force the clerk to update the password at the next sign-on.
63	VIOLATION FLAG	The violation flag indicates the password status on the Clerk Record Update (CLRK) Screen. If a clerk's password has been violated (keyed incorrectly 3 times in a row), the value is Y. The value of Y prevents MCS sign-on for the clerk number. The other valid value is N, which means that no violation has occurred. When the password is reset or changed, the system resets this field to R.
64	PROD MODE AUTHORIZATION	Authorization to sign on to MCS in a production (versus test) mode. Valid values are N and Y.
65	MSG	System generated error/informational message.

APPENDIX E - VMS SECURITY EXPRESS SCREEN4 EXAMPLE

Figure 10 VMS Security Express Screen

```
________                    SECURITY EXPRESS SCREEN                    VMSSE07

USER ID: 0000000   LINDA-W
DEPT ID: CARR      CARRIER

SWITCHES   1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0
001 - 030  Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y N Y Y Y Y Y Y Y Y Y Y
031 - 060  Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y
061 - 090  Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y N N N
091 - 120  Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y
121 - 150  Y Y N N N N N N N N N N N N N N N N N N N N N N N N N N N N
151 - 180  Y Y Y Y Y Y Y Y N N N N N Y N N N N N N N N N N N N Y Y Y Y
181 - 210  Y N N N N N N N Y Y Y Y N N Y Y Y N Y Y Y Y Y Y N Y Y Y Y Y
211 - 240  Y N N N Y Y Y Y Y Y N N N N N N N N N Y Y Y Y Y Y Y Y Y Y Y
241 - 270  Y Y N Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y N N N N N N N N N
271 - 300  N Y Y Y Y N N N N N N N N N N Y Y Y Y Y Y N Y Y N Y N N N
301 - 330  N N N N N Y N N Y N Y Y Y Y N N N N N Y Y Y N N N N N N N Y
331 - 360  Y Y Y N Y Y Y Y N Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y
361 - 390  Y N N N N N N N N Y N N Y Y Y Y Y Y N N N Y Y Y N N N N N N
391 - 420  N N Y N N N Y N N N N Y N N N Y Y N N Y Y Y Y Y N N N N N N
421 - 450  N N N N N N Y Y Y N Y Y N N N Y Y N N N N N N N N N Y N N N
451 - 480  N N N N N N N N N N N N N N N N Y Y Y Y Y Y Y Y Y Y Y N Y N
481 - 510  Y N N Y N N N N N N N N N N N N N N Y N N N N N Y N N N N
```

Table 6 VMS Security Express Security Switch Values

Security Switch Values Sorted by Switch Number				
Switch #	Tran ID	Question #	Question Text	Values
001	ACES	01	Authority for this Transaction	N No authority for this transaction Y Authority to access for all EAR types
002	ADST1	01	Authority for this Transaction	N No authority for this transaction Y Authority to access for ADST/1 (MSP Claim Action)
003	ADST3	01	Authority for this Transaction	N No authority for this transaction Y Authority to access for ADST/3 (ADS Claim Action)
004	ADST4	01	Authority for this Transaction	N No authority for this transaction Y Authority to access for ADST/4 (ADS Development Status)
005	APEX1	01	Authority for this Transaction	N No authority for this transaction Y Authority to access for APEX/1 (APEX Suspense Claim Processing)
006	APEX2	01	Authority for this Transaction	N No authority for this transaction Y Authority to access for APEX/2 (APEX Print Options Screen)
007	APEX3	01	Authority for this Transaction	N No authority for this transaction Y Authority to access for APEX/3 (APEX Claim Loc/Status Query)

[4] Information was obtained from the ViPS VMS Security (VSEC) User Guide, Revision 2006-2/April, Chapter 3 and Appendix C

Security Switch Values Sorted by Switch Number				
008	APEX4	01	Authority for this Transaction	N No authority for this transaction Y Authority to access for APEX/4 (APEX Total Location/Status)
009	APPL1	01	Authority for this Transaction	N No authority for this transaction Y Authority to access for APPL/1 (Provider Subsystem)
010	APPL2 APPL/D	01	Authority for this Transaction	N No authority for this transaction Y Authority to access for APPL/2 (Area Prevailing)
011	APPL3	01	Authority for this Transaction	N No authority for this transaction Y Authority to access APPL/3 (Provider Cross Reference System)
012	APPL4	01	Authority for this Transaction	N No authority for this transaction Y Authority to access APPL/4 (Master Procedure/ Diagnosis Record System)
013	APPL5	01	Authority for this Transaction	N No authority for this transaction Y Authority to access APPL/5 (Physician Payment Reform)
014				Reserved for future use
015	APPL7	01	Authority for this Transaction	N No authority for this transaction Y Authority to access APPL/7 (Mammography Cert)
016	APPL8	01	Authority for this Transaction	N No authority for this transaction Y Authority to access APPL/8 (Provider Cross Reference)
017	APPL9	01	Authority for this Transaction	N No authority for this transaction Y Authority to access APPL/9 (Ambulance)
018	ARUC1	01	Authority for this Transaction	N No authority for this transaction Y Authority to access the beneficiary ARU (Audio Response Unit) screens
019	ARUC2	01	Authority for this Transaction	N No authority for this transaction Y Authority to access the provider ARU (Audio Response Unit) screens
020	BITSPA	01	Authority for this Transaction	N No authority for this transaction Y Authority to access BITS (Beneficiary Information Tracking System)
021	BMAN	01	Authority for this Transaction	N No authority for this transaction Y Authority to access BMAN (Batch Manager)
022	BUDS00	01	Authority for this Transaction	N No authority for this transaction Y Authority to access BUDS/00 (Medicare Reporting System)
023	BUDS01	01	Authority for this Transaction	N No authority for this transaction Y Authority to access BUDS/01 (Beneficiary Information)
024	BUDS02	01	Authority for this Transaction	N No authority for this transaction Y Authority to access BUDS/02 (Beneficiary Information/MSP)

Security Switch Values Sorted by Switch Number				
025	BUDS03	01	Authority for this Transaction	N No authority for this transaction Y Authority to access BUDS/03 (Claim History Header)
026	BUDS04	01	Authority for this Transaction	N No authority for this transaction Y Authority to access BUDS/04 (Claim History Full Lines)
027	BUDS05	01	Authority for this Transaction	N No authority for this transaction Y Authority to access BUDS/05 (Claim History Base Lines)
028	BUDS06	01	Authority for this Transaction	N No authority for this transaction Y Authority to access BUDS/06 (Line Item History)
029	BUDS07	01	Authority for this Transaction	N No authority for this transaction Y Authority to access BUDS/07 (Summary Claim History)
030	BUDS08	01	Authority for this Transaction	N No authority for this transaction Y Authority to access BUDS/08 (Primary Detail Claim History)
031	BUDS09	01	Authority for this Transaction	N No authority for this transaction Y Authority to access BUDS/09 (Financial Claim History)
032	BUDS10	01	Authority for this Transaction	N No authority for this transaction Y Authority to access BUDS/10 (Expanded MSP Information)
033	BUDS11	01	Authority for this Transaction	N No authority for this transaction Y Authority to access BUDS/11 (Beneficiary Name Search)
034	BUDS12	01	Authority for this Transaction	N No authority for this transaction Y Authority to access BUDS/12 (Beneficiary HICN Search)
035	BUDS13	01	Authority for this Transaction	N No authority for this transaction Y Authority to access BUDS/13 (NSF Inquiry)
036	BUDS14	01	Authority for this Transaction	N No authority for this transaction Y Authority to access BUDS/14 (Competitive Bid Beneficiary Information)
037	BUDS15	01	Authority for this Transaction	N No authority for this transaction Y Authority to access BUDS/15 (Beneficiary Profile)
038	BUDS16	01	Authority for this Transaction	N No authority for this transaction Y Authority to access BUDS/16 (VMS/HIMR Bene MSP Summary)
039	BUDS20	01	Authority for this Transaction	N No authority for this transaction Y Authority to access BUDS/20 (Demo Census Record)
040	BUDS21	01	Authority for this Transaction	N No authority for this transaction Y Authority to access BUDS/21 (Claim History Claim List)

Security Switch Values Sorted by Switch Number				
041	BUDS22	01	Authority for this Transaction	N No authority for this transaction Y Authority to access BUDS/22 (Provider Name Search)
042	BUDS23	01	Authority for this Transaction	N No authority for this transaction Y Authority to access BUDS/23 (Remittance Detail)
043	BUDS24	01	Authority for this Transaction	N No authority for this transaction Y Authority to access BUDS/24 (Remittance Summary)
044	BUDS25	01	Authority for this Transaction	N No authority for this transaction Y Authority to access BUDS/25 (Crossover Activity)
045	BUDS26	01	Authority for this Transaction	N No authority for this transaction Y Authority to access BUDS/26 (Other Carrier Name/Address)
046	BUDS27	01	Authority for this Transaction	N No authority for this transaction Y Authority to access BUDS/27 (Provider Check History)
047	BUDS28	01	Authority for this Transaction	N No authority for this transaction Y Authority to access BUDS/28 (Secondary Claim History Detail)
048	BUDS29	01	Authority for this Transaction	N No authority for this transaction Y Authority to access BUDS/29 (Other Carrier Name Lookup)
049	BUDS30	01	Authority for this Transaction	N No authority for this transaction Y Authority to access BUDS/30 (PIMR Prepay MR Detail)
050	CHIP03	01	Authority for this Transaction	N No authority for this transaction Y Authority to access CHIP/03 (Claim History Header)
051	CHIP04	01	Authority for this Transaction	N No authority for this transaction Y Authority to access CHIP/04 (Claim History Full Lines)
052	CHIP05	01	Authority for this Transaction	N No authority for this transaction Y Authority to access CHIP/05 (Claim History Base Lines)
053	CHIP06	01	Authority for this Transaction	N No authority for this transaction Y Authority to access CHIP/06 (Claim Line Item History)
054	CHIP07	01	Authority for this Transaction	N No authority for this transaction Y Authority to access CHIP/07 (Summary Claim History)
055	CHIP08	01	Authority for this Transaction	N No authority for this transaction Y Authority to access CHIP/08 (Primary Detail Claim History)
056	CHIP09	01	Authority for this Transaction	N No authority for this transaction Y Authority to access CHIP/09 (Financial Claim History)

Security Switch Values Sorted by Switch Number				
057	CHIP21	01	Authority for this Transaction	N No authority for this transaction Y Authority to access CHIP/21 (Claim History Claim List)
058	CHIP22	01	Authority for this Transaction	N No authority for this transaction Y Authority to access CHIP/22 (Provider Name Search)
059	CHIP23	01	Authority for this Transaction	N No authority for this transaction Y Authority to access CHIP/23 (Remittance Detail)
060	CHIP24	01	Authority for this Transaction	N No authority for this transaction Y Authority to access CHIP/24 (Remittance Summary)
061	CHIP27	01	Authority for this Transaction	N No authority for this transaction Y Authority to access CHIP/27 (Provider Check History)
062	CHIP28	01	Authority for this Transaction	N No authority for this transaction Y Authority to access CHIP/28 (Secondary Detail Claim History)
063	COIN1	01	Authority for this Transaction	N No authority for this transaction Y Authority to access COIN/01 (Complementary Insurance Header Record)
064	COIN2	01	Authority for this Transaction	N No authority for this transaction Y Authority to access COIN/02 (Complementary Insurance Beneficiary List Screen)
065				Reserved for future use
066	HARP	01	Authority for this Transaction	N No authority for this transaction Y Authority to access HARP (HCPCS Auto Revision Process)
067	ICOR	01	Authority for this Transaction	N No authority for this transaction Y Authority to access ICOR (Interactive Correspondence Online Reporting)
068	LTRO	01	Authority for this Transaction	N No authority for this transaction Y Authority to access LTRO (Letter Writer)
069	APPL/C	01	Authority for this Transaction	N No authority for this transaction Y Authority to access APPL/C (Drug Pricing)
070	MGTP	01	Authority for this Transaction	N No authority for this transaction Y Authority to access MGTP (Medicare Biller Control File)
071	MICR	01	Authority for this Transaction	N No authority for this transaction Y Authority to access MICR (Microfilmed Documentation Requests)
072	MONI	01	Authority for this Transaction	N No authority for this transaction Y Authority to access MONI (Money Online Notification and Inquiry)

Security Switch Values Sorted by Switch Number				
073	MONIB	01	Authority for this Transaction	N No authority for this transaction Y Authority to access MONI Check Reconciliation
074	MONIK	01	Authority for this Transaction	N No authority for this transaction Y Authority to access MONI/K (MONI Check Log)
075	MSSG	01	Authority for this Transaction	N No authority for this transaction Y Authority to access MSSG (Message File Maintenance)
076	OLDE	01	Authority for this Transaction	N No authority for this transaction Y Authority to access OLDE (Online Documentation System)
077	BUDS19	01	Authority for this Transaction	N No authority for this transaction Y Authority to access BUDS/19 (PIMR Audit Record History)
078	APPL/A	01	Authority for this Transaction	N No authority for this transaction Y Authority to access APPL/A (Clinical Lab Subsystem)
079	OLDF	01	Authority for this Transaction	N No authority for this transaction Y Authority to access OLDF (OLDS File Selection Menu)
080	OLDS	01	Authority for this Transaction	N No authority for this transaction Y Authority to access OLDS (OLDS Selection Menu)
081	OLDV	01	Authority for this Transaction	N No authority for this transaction Y Authority to access OLDV (OLDS Environment Maintenance)
082	PENS	01	Authority for this Transaction	N No authority for this transaction Y Authority to access PENS (Provider Enrollment System)
083	PINQ	01	Authority for this Transaction	N No authority for this transaction Y Authority to access PINQ/VPIQ (Provider Inquiry System)
084	PRS1	01	Authority for this Transaction	N No authority for this transaction Y Authority to access Provider Criteria Report Selection
085	STAT	01	Authority for this Transaction	N No authority for this transaction Y Authority to access your own Terminal Operator Statistics
086	SUPR	01	Authority for this Transaction	N No authority for this transaction Y Authority to access SuperOp
087	TCLM	01	Authority for this Transaction	N No authority for this transaction Y Authority to access TCLM
088	VANSCL	01	Authority for this Transaction	N No authority for this transaction Y Authority to access VANS claims data screens
089	VANSPE	01	Authority for this Transaction	N No authority for this transaction Y Authority to access VANS parameters and edits screens

Security Switch Values Sorted by Switch Number				
090	VANSSB	01	Authority for this Transaction	N No authority for this transaction Y Authority to access VANS submitter data screens
091				Reserved for future use
092	VCAP	01	Authority for this Transaction	N No authority for this transaction Y Authority to access VCAP (ViPS CMN APEX)
093	VCHK1	01	Authority for this Transaction	Empire only N No authority for this transaction Y Authority to access the Payee/Provider subsystem of the Checkmate system
094	VCHK2	01	Authority for this Transaction	Empire only N No authority for this transaction Y Authority to access the Rule Maintenance subsystem of the Checkmate system
095	VCHK3	01	Authority for this Transaction	Empire only N No authority for this transaction Y Authority to access the Alert Review subsystem of the Checkmate system
096	VCHK4	01	Authority for this Transaction	Empire only N No authority for this transaction Y Authority to access the Carrier Maintenance subsystem of the Checkmate system
097	VCMN	01	Authority for this Transaction	DMERC only N No authority for this transaction Y Authority to access the VCMN Display and Update system
098	VDME	01	Authority for this Transaction	DMERC only N No authority for this transaction Y Authority to access DMERC CMN Processing
099	VCOB	01	Authority for this Transaction	N No authority for this transaction Y Authority to access VCOB
100	VEC9	01	Authority for this Transaction	N No authority for this transaction Y Authority to access Entry Code Nine
101	VEIN	01	Authority for this Transaction	N No authority for this transaction Y Authority to access VEIN
102	VLGM	01	Authority for this Transaction	N No authority for this transaction Y Authority to access VLGM/VLGS (ViPS Letter Generating Maintenance/ ViPS Letter Generating System)
103	APPL/B	01	Authority for this Transaction	N No authority for this transaction Y Authority to access the HPSA/PSA screens for inquiry
104	VMAP1	01	Authority for this Transaction	N No authority for this transaction Y Authority to access VMAP/1 (Contractor Options)

Security Switch Values Sorted by Switch Number				
105	VMAP2	01	Authority for this Transaction	N No authority for this transaction Y Authority to access VMAP/2 (QAOS)
106	VMAP3	01	Authority for this Transaction	N No authority for this transaction Y Authority to access VMAP/3 (Control Options)
107	VMAP4	01	Authority for this Transaction	N No authority for this transaction Y Authority to access VMAP/4 (System Parameters)
108	VMAP5	01	Authority for this Transaction	N No authority for this transaction Y Authority to access VMAP/5 (Rebundling System)
109	VMAP6	01	Authority for this Transaction	N No authority for this transaction Y Authority to access VMAP/6 (Pre-Payment Utilization Options)
110	VMAP7	01	Authority for this Transaction	N No authority for this transaction Y Authority to access VMAP/7 (Claim History Reporting Sub-System)
111	VMON	01	Authority for this Transaction	N No authority for this transaction Y Authority to access VMON (ViPS Medicare Claim System)
112	VNOT	01	Authority for this Transaction	N No authority for this transaction Y Authority to access VNOT (Notepad)
113	VOQC	01	Authority for this Transaction	N No authority for this transaction Y Authority to access VOQC (Online Quality Control)
114	VPLD	01	Authority for this Transaction	N No authority for this transaction Y Authority to access VPLD (ViPS Load)
115	BUDS31	01	Authority for this Transaction	N No authority for this transaction Y Authority to access BUDS31 (LMRP/NCD Record History)
116				Reserved for future use
117				Reserved for future use
118	VSAF	01	Authority for this Transaction	N No authority for this transaction Y Authority to access VSAF (SAFE)
119	VTFS	01	Authority for this Transaction	N No authority for this transaction Y Authority for FEPI flight simulator testing
120	VTPD	01	Authority for this Transaction	N No authority for this transaction Y Authority to maintain FEPI pool definitions
121	XADJ	01	Authority for this Transaction	N No authority for this transaction Y Authority to access XADJ (Express Adjustments)
122	XLST	01	Authority for this Transaction	N No authority for this transaction Y Authority to access XLST (Transaction List Menu)
123				Reserved for future use
124				Reserved for future use
125				Reserved for future use

Security Switch Values Sorted by Switch Number				
126				Reserved for future use
127				Reserved for future use
128				Reserved for future use
129				Reserved for future use
130				Reserved for future use
131				Reserved for future use
132				Reserved for future use
133				Reserved for future use
134				Reserved for future use
135				Reserved for future use
136				Reserved for future use
137				Reserved for future use
138				Reserved for future use
139				Reserved for future use
140				Reserved for future use
141				Reserved for future use
142				Reserved for future use
143				Reserved for future use
144				Reserved for future use
145				Reserved for future use
146				Reserved for future use
147				Reserved for future use
148				Reserved for future use
149				Reserved for future use
150				Reserved for future use
151	ACES	02	Maintain Carrier EARs	N No authority for this transaction Y Add/update authority for carrier and non-specific EARs (types 21, 41, 51; 29, 49, 59)
152	ACES	03	Maintain Beneficiary EARs	N No authority for this transaction Y Add/update authority for beneficiary and non-specific EARs (types 22, 42, 52; 29, 49, 59)
153	ACES	04	Maintain Provider EARS	N No authority for this transaction Y Add/update authority for provider and non-specific EARs (types 23, 43, 53; 24, 44, 54; 27, 47, 57; 29, 49, 59)
154	ACES	05	Maintain Examiner EARs	N No authority for this transaction Y Add/update authority for examiner and non-specific EARs (types 25, 45, 55; 29, 49, 59)
155	ACES	06	Maintain Procedure EARs	N No authority for this transaction Y Add/update authority for procedure and non-specific EARs (types 26, 49, 59; 29, 49, 59)

Security Switch Values Sorted by Switch Number				
156	ACES	07	Maintain Referring UPIN EARs	N No authority for this transaction Y Add/update authority for referring UPIN and non-specific EARs (types 27, 47, 57; 29, 49, 59)
157	ACES	08	Maintain Non-specific EARs	N No authority for this transaction Y Add/update authority for non-specific EARs (types 29, 49, 59)
158	ACES	09	Maintain DMERC CMN Grid EARs	N No authority for this transaction Y Add/update authority for DMERC CMN Grid EARs (type 25)
159	VCHK4	06	Update TimeCheck Procedure Codes	Empire only N No authority for this transaction Y Authority to update TimeCheck procedure codes
160	VCHK4	07	Delete TimeCheck Procedure Codes	Empire only N No authority for this transaction Y Authority to delete TimeCheck procedure codes
161	VCHK4	04	Update TimeCheck Action Codes	Empire only N No authority for this transaction Y Authority to update TimeCheck action codes
162	VCHK4	05	Delete TimeCheck Action Codes	Empire only N No authority for this transaction Y Authority to delete TimeCheck action codes
163	VMON	12	Copy Claims Authority	N No authority for this transaction Y Authority to copy claims
164	VMON	13	Data-Entry Claims Authority	N No authority for this transaction Y Authority to access VMON as a Data Entry operator
165	VMON	14	Training Claims Authority	N No authority for this transaction Y Authority to access VMON as a Training operator
166	VMON	15	Delete Claims Authority	N No authority for this transaction Y Authority to delete claims
167	VMON	16	Update CWF Override Group B	N No authority for this transaction Y Authority to update CWF Override Group B (D930)
168	VMON	17	Update CWF Override Group C	N No authority for this transaction Y Authority to update CWF Override Group C (5512)
169	VMON	18	Update NCD Override	N No authority for this transaction Y Authority to enter Y or Space in Override Indicator field
170	VMON	19	Update CWF Override Group D	N No authority for this transaction Y Authority to update CWF Override Group D (DA02, DA05, DA06, DA07, DA09, 7294). DMERC-only switch.

Security Switch Values Sorted by Switch Number				
171	VMON	20	Update CWF Override Group E	N No authority for this transaction Y Authority to update CWF Override Group E (5412, 5413, 8022, 8024). MEDB-only switch.
172	APPL/C	02	Update Drug Fee Schedule	N No authority for this transaction Y Authority to update the Drug Fee Schedule
173	APPL/C	03	Add Drug Fee Schedule	N No authority for this transaction Y Authority to add a new Drug Fee Schedule
174	APPL/C	04	Delete Drug Fee Schedule	N No authority for this transaction Y Authority to delete a Drug Fee Schedule
175	APPL/C	05	Generate Drug Fee Reports	N No authority for this transaction Y Authority to generate Drug Fee reports
176	APPL/C	06	Update Drug Fee Schedule Pricing Period	N No authority for this transaction Y Authority to update Drug Fee Schedule Pricing Periods
177	ADST1	02	Maintain MSP Claim Action Table	N No authority for this transaction Y Update authority for the MSP Claim Action table
178	ADST3	02	Maintain ADS Claim Action Table	N No authority for this transaction Y Update authority for the ADS Claim Action table
179	ADST4	02	Maintain ADS Development Table	N No authority for this transaction Y Update authority for the ADS Development table
180	APEX1	02	Totals	N No authority for this transaction Y Update authority for APEX totals
181	APEX1	03	Reprocess	N No authority for this transaction Y Update authority for APEX reprocessing
182	APEX1	04	Update Team Action	N No authority for this transaction Y Update the APEX Request Screen TEAM field
183	APEX1	05	Delete Claims	N No authority for this transaction Y Authority to delete claims from APEX
184				Reserved for future use
185				Reserved for future use
186				Reserved for future use
187				Reserved for future use
188				Reserved for future use
189	APEX2	02	Print Options	N No authority for this transaction Y Update authority for the APEX Print Options screen
190	APPL1	02	Update Provider Header	N No authority for this transaction Y Update authority for the Provider Header1 and Provider Header2 screens

Security Switch Values Sorted by Switch Number				
191	APPL1	03	Add Provider Header	N No authority for this transaction Y Add authority for the Provider Header1 and Provider Header2 screens Note: For MedB carriers, this switch only applies in test mode.
192	APPL1	04	Delete Provider Header	N No authority for this transaction Y Delete authority for the Provider Header1 and Provider Header2 screens Note: For MedB carriers, this switch only applies in test mode.
193	APPL1	05	Update Provider Header except Name and Address	N No authority for this transaction Y Update authority for the Provider Header1 and Provider Header2 screens except for the Name and Address fields Note: For MedB carriers, this switch only applies in test mode.
194	APPL1	06	Copy Provider Header	N No authority for this transaction Y Copy authority for the Provider Header1 and Provider Header2 screens Note: For MedB carriers, this switch only applies in test mode.
195	APPL1	07	Update Abbreviated Customary	N No authority for this transaction Y Update authority for Provider Abbreviated Customary screen
196	APPL1	08	Add Abbreviated Customary	N No authority for this transaction Y Add authority for the Provider Abbreviated Customary screen
197	APPL1	32	Update Flag A	N No authority for this transaction Y Authority to update Flag A (DMERC "dummy" supplier indicator)
198	APPL1	09	Copy Abbreviated Customary	N No authority for this transaction Y Copy authority for the Provider Abbreviated Customary screen
199	APPL1	33	Update Paper Claim Deny Detail Record	N No authority for this transaction Y Authority to update Paper Claim Deny Detail Record
200	APPL1	34	Add Paper Claim Deny Detail Record	N No authority for this transaction Y Authority to add Paper Claim Deny Detail Record
201	APPL1	35	Delete Paper Claim Deny Detail Record	N No authority for this transaction Y Authority to delete Paper Claim Deny Detail Record
202				Reserved for future use
203				Reserved for future use
204				Reserved for future use
205				Reserved for future use

Security Switch Values Sorted by Switch Number				
206	APPL1	14	Update Provider Withholding	N No authority for this transaction Y Update authority for the 1099 Withholding Inquiry/Update screen
207				Reserved for future use
208				Reserved for future use
209				Reserved for future use
210	APPL1	18	Update Base Quarter Charges	N No authority for this transaction Y Update authority for the BQTR field on the Provider Abbreviated Customary screen
211	APPL1	19	Request Customary PIDS Reports	N No authority for this transaction Y Authority to request the Customary PIDS reports
212	APPL1	20	Update Alert Codes	N No authority for this transaction Y Update authority for the Alert Code Inquiry/Update screen
213	APPL1	21	Add Alert Codes	N No authority for this transaction Y Add authority for the Alert Code Inquiry/Update screen
214	APPL1	22	Delete Alert Codes	N No authority for this transaction Y Delete authority for the Alert Code Inquiry/Update screen
215	APPL1	23	Maintain EFT	N No authority for this transaction Y Update authority for the EFT Banking Inquiry/Update screen
216	APPL1	24	Update DMERC Provider Specialty Codes	N No authority for this transaction Y Update authority for the DMERC Provider Specialty Inquiry/Update screen
217	APPL1	25	Add DMERC Provider Specialty Codes	N No authority for this transaction Y Update authority for the SPEC field on the DMERC Provider Specialty Inquiry/Update screen
218	APPL1	26	Update DMERC Supplier Comp Bid Records	N No authority for this transaction Y Update authority for the DMERC Competitive Bid Supplier Detail screen
219	APPL1	27	Add DMERC Suppler Comp Bid Records	N No authority for this transaction Y Add authority for the DMERC Competitive Bid Supplier Detail screen
220	APPL1	28	Delete DMERC Supplier Comp Bid Records	N No authority for this transaction Y Delete authority for the DMERC Competitive Bid Supplier Detail screen
221	APPL/A	02	Update Clinical Lab Fee Schedule	N No authority for this transaction Y Update authority for the Clinical Lab Fee Schedule
222	APPL/A	03	Add Clinical Lab Fee Schedule	N No authority for this transaction Y Update authority for the Clinical Lab Fee Schedule

Security Switch Values Sorted by Switch Number				
223	APPL/A	04	Delete Clinical Lab Fee Schedule	N No authority for this transaction Y Delete authority for the Clinical Lab Fee Schedule
224	APPL/A	05	Generate Clinical Lab Fee Schedule Reports	N No authority for this transaction Y Authority to generate the Clinical Lab Fee Schedule reports
225	APPL1	30	Allow MEDB Add/Update	N No authority for this transaction Y Update authority for Provider file non-enrollment fields Note: To enable the update, turn on either switch 190 or 193 before using this switch (225).
226	APPL1	31	Allow PECOS Holding File Updates	N No authority for this transaction Y Update authority for PECOS Holding files for non-enrollment fields
227	APPL/A	06	Update Clinical Lab Fee Schedule Pricing Years	N No authority for this transaction Y Update authority for the Clinical Lab Fee Schedule Pricing Years screen
228				Reserved for future use
229				Reserved for future use
230				Reserved for future use
231	APPL2	02	Update 75th and 50th	N No authority for this transaction Y Update authority for the Area Prevailing 75th/50th
231	APPL/D	02	Update DMEPOS/PEN Fee Schedule	N No authority for this transaction Y Update authority for the DMEPOS/PEN fee schedule
232	APPL2	03	Add 75th and 50th	N No authority for this transaction Y Add authority for the Area Prevailing 75th/50th
232	APPL/D	03	Add DMEPOS/PEN Fee Schedule	N No authority for this transaction Y Add authority for the DMEPOS/PEN fee schedule
233	VMAP3	03	Update Status Criteria	N No authority for this transaction Y Authority to update Status Criteria
234	APPL2	04	Update LCL/IIC	N No authority for this transaction Y Update authority for the Area Prevailing LCL (lowest charge levels) and IIC (inflation indexed charge)
234	APPL/D	04	Update DMEPOS/PEN Floor/ Ceiling	N No authority for this transaction Y Update authority for the DMEPOS/PEN Floor/ Ceiling fields
235	APPL2	05	Add LCL/IIC	N No authority for this transaction Y Add authority for the Area Prevailing LCL (lowest charge levels) and IIC (inflation indexed charge)
235	APPLD	05	Add DMEPOS/PEN Floor/Ceiling	N No authority for this transaction Y Add authority for the DMEPOS/PEN Floor/ Ceiling fields

Security Switch Values Sorted by Switch Number				
236	VMAP3	04	Update Batch Activation Range	N No authority for this transaction Y Authority to update the Batch Activation Range
237	APPL2	06	Update Conversion Factors	N No authority for this transaction Y Update authority for the Area Prevailing conversion factors
237	APPL/D	06	Update DMEPOS/PEN Pricing Period	N No authority for this transaction Y Update authority for the DMEPOS/PEN Pricing Period
238	APPL2	07	Add Conversion Factors	N No authority for this transaction Y Add authority for the Area Prevailing conversion factors
239	VMAP3	05	Control Delete Function	N No authority for this transaction Y Authority to control the Delete Function
240	APPL2	08	Request Area Prevailing Report	N No authority for this transaction Y Authority to request the Area Prevailing report
240	APPL/D	08	Request DMEPOS/PEN Reports	N No authority for this transaction Y Authority to request the DMPOS/PEN reports
241	APPL3	02	Update/Delete Provider XREF	N No authority for this transaction Y Update/delete authority for APPL/3 (Provider Cross Reference System)
242	APPL3	03	Add/Delete Provider XREF	N No authority for this transaction Y Add/delete authority for APPL/3 (Provider Cross Reference System)
243				Reserved for future use
244	APPL4	02	Update MPRs	N No authority for this transaction Y Update authority for Master Procedure Records
245	APPL4	03	Add MPRs	N No authority for this transaction Y Add authority for Master Procedure Records
246	APPL4	04	Delete MPRs	N No authority for this transaction Y Delete authority for Master Procedure Records
247	APPL4	05	Update Proc Descriptions	N No authority for this transaction Y Update authority for procedure descriptions
248	APPL4	06	Add Proc Descriptions	N No authority for this transaction Y Add authority for procedure descriptions
249	APPL4	07	Delete Proc Descriptions	N No authority for this transaction Y Delete authority for procedure descriptions
250	APPL4	08	Update Diagnosis Sets	N No authority for this transaction Y Update authority for diagnosis sets
251	APPL4	09	Add Diagnosis Sets	N No authority for this transaction Y Update authority for diagnosis sets

Security Switch Values Sorted by Switch Number				
252	APPL4	10	Delete Diagnosis Sets	N No authority for this transaction Y Update authority for diagnosis sets
253	APPL4	11	Update Diagnosis Records	N No authority for this transaction Y Update authority for diagnosis records
254	APPL4	12	Add Diagnosis Records	N No authority for this transaction Y Add authority for diagnosis records
255	APPL4	13	Delete Diagnosis Records	N No authority for this transaction Y Delete authority for diagnosis records
256	APPL4	14	Update MPR Diagnosis	N No authority for this transaction Y Update authority for MPR diagnosis
257	APPL4	15	Add MPR Diagnosis	N No authority for this transaction Y Add authority for MPR diagnosis
258	APPL4	16	Delete MPR Diagnosis	N No authority for this transaction Y Delete authority for MPR diagnosis
259	APPL4	17	Update NDC Records	N No authority for this transaction Y Update authority for NDC (National Drug Code) records
260	APPL4	18	Add NDC Records	N No authority for this transaction Y Add authority for NDC (National Drug Code) records
261	APPL4	19	Delete NDC Records	N No authority for this transaction Y Delete authority for NDC (National Drug Code) records
262				Reserved for future use
263				Reserved for future use
264				Reserved for future use
265				Reserved for future use
266				Reserved for future use
267				Reserved for future use
268				Reserved for future use
269				Reserved for future use
270				Reserved for future use
271				Reserved for future use
272	APPL5	02	Update MPFSDB	N No authority for this transaction Y Update authority for the MPFSDB (Medicare Physician Fee Schedule Database)
273	APPL5	03	Add MPFSDB	N No authority for this transaction Y Add authority for the MPFSDB (Medicare Physician Fee Schedule Database)
274	APPL5	04	Delete MPFSDB	N No authority for this transaction Y Delete authority for the MPFSDB (Medicare Physician Fee Schedule Database)
275	APPL5	05	Request PIDS Report	N No authority for this transaction Y Authority to request the PIDS Report
276				Reserved for future use

Security Switch Values Sorted by Switch Number				
277				Reserved for future use
278				Reserved for future use
279				Reserved for future use
280				Reserved for future use
281				Reserved for future use
282				Reserved for future use
283				Reserved for future use
284				Reserved for future use
285				Reserved for future use
286				Reserved for future use
287	APPL7	02	Update Mammography Certification Records	N No authority for this transaction Y Update authority for mammography certificate records
288	APPL7	03	Add Mammography Certification Records	N No authority for this transaction Y Add authority for mammography certificate records
289	APPL7	04	Delete Mammography Certification Records	N No authority for this transaction Y Delete authority for mammography certificate records
290	APPL9	02	Update Ambulance Fee Schedule	N No authority for this transaction Y Update authority for the Ambulance Fee Schedule
291	APPL9	03	Add Ambulance Fee Schedule	N No authority for this transaction Y Add authority for the Ambulance Fee Schedule
292	APPL9	04	Delete Ambulance Fee Schedule	N No authority for this transaction Y Delete authority for the Ambulance Fee Schedule
293	APPL9	05	Generate AFS Reports	N No authority for this transaction Y Authority to generate the Ambulance Fee Schedule reports
294	APPL9	06	Update Ambulance Pricing Years	N No authority for this transaction Y Update authority for the Ambulance Pricing Years screen
295	APPL9	07	Maintain Ambulance ZIP Code	N No authority for this transaction Y Update authority for the Ambulance ZIP Code screen
296	VDME	08	Update CMN Status	DMERC only N No authority for this transaction Y Authority to update CMN statuses
297				Reserved for future use
298	APPL9	07	Maintain Ground Transport Bonus Screen	N No authority for this transaction Y Update authority for the Ambulance Ground Transport Bonus screen
299				Reserved for future use
300				Reserved for future use
301				Reserved for future use
302				Reserved for future use

Security Switch Values Sorted by Switch Number				
303				Reserved for future use
304				Reserved for future use
305	BITSPA	02	Maintain Prior Authorization	N No authority for this transaction Y Authority to maintain prior authorization in BITS (Beneficiary Information Tracking System)
306	VMAP4	15	VMAP/4C Maintain Pricing Year Table	N No authority for this transaction Y Authority to maintain the VMAP/4C Pricing Year table
307	BMAN	02	Update your own Batch Ranges	N No authority for this transaction Y Authority to update your own batch ranges in BMAN (Batch Manager)
308	BMAN	03	Update any Batch Ranges	N No authority for this transaction Y Authority to update any batch range in BMAN (Batch Manager)
309	BUDS01	04	Update Bene Name and Demographic Fields	N No authority for this transaction Y Authority to update beneficiary name and demographic fields (name; sex; rep payee name and type; beneficiary address 1, 2, and 3; city, state; ZIP; and phone)
310	BUDS01	08	Update BSC Indicator	N No authority for this transaction Y Authority to update the BUDS01 BSC (Beneficiary Submitted Claim) indicator
311	BUDS01	02	Update Comp Code Fields	N No authority for this transaction Y Authority to update comp code fields (comp code, number, to/from dates) and beneficiary phone number field
312	BUDS01	05	Full Update except XREF Fields	N No authority for this transaction Y Authority for full update except XREF fields (bene name and demographic fields; comp code fields; Medicaid code and number; query indicator; UT indicator; overpay indicator and reimbursement method – current/previous; CRD dates – current/ previous; HMO fields, death dates; status – close and reopen capability only)
313	BUDS01	06	Full Update and XREF Fields	N No authority for this transaction Y Authority for full update for comp code, demographics, full update, x-ref fields (allows all of the updates in questions 02, 03, 04) to update comp code fields (comp code, number, to/from dates) and beneficiary phone number field
314	BUDS01	03	Update Scrub Indicator	N No authority for this transaction Y Authority to update the SCRUB field on BUDS01

Security Switch Values Sorted by Switch Number				
315	BUDS01	07	Update CRD field	N No authority for this transaction Y Authority to update the CRD field on BUDS01
316				Reserved for future use
317				Reserved for future use
318				Reserved for future use
319				Reserved for future use
320	BUDS02	02	Maintain Bene MSP Occurrences	N No authority for this transaction Y Authority to maintain beneficiary MSP occurrences on BUDS/02 (Beneficiary Information/MSP)
321	BUDS02	03	Delete MSP Occurrences	N No authority for this transaction Y Authority to delete MSP occurrences on BUDS/02
322				Reserved for future use
323				Reserved for future use
324				Reserved for future use
325				Reserved for future use
326				Reserved for future use
327				Reserved for future use
328				Reserved for future use
329				Reserved for future use
330	BUDS10	02	Update Bene MSP Occurrence	N No authority for this transaction Y Authority to update beneficiary MSP occurrences on BUDS/10
331	BUDS15	02	Update Bene Name and Demographic Fields	N No authority for this transaction Y Authority to update beneficiary name and demographic fields (name; sex; rep payee name and type; beneficiary address 1, 2, and 3; city, state; ZIP; and phone)
332	VOQC	02	Supervisor	N No authority for this transaction Y Authority to access VOQC (Online Quality Control) as a supervisor
333	BUDS15	03	Question #2 Plus Full Update except XREF Fields	N No authority for this transaction Y Switch 331 authority and authority for full update except XREF fields (bene name and demographic fields; comp code fields; Medicaid code and number; query indicator; UT indicator; overpay indicator and reimbursement method – current/previous; CRD dates – current/ previous; HMO fields, death dates; status – close and reopen capability only)
334	VOQC	03	Pend-Review-only	N No authority for this transaction Y Authority to review pending claims only

Security Switch Values Sorted by Switch Number				
335	BUDS15	04	Question #2 Plus Full Update and XREF Fields	N No authority for this transaction Y Switch 331 authority and authority for full update to comp code, demographics, full update, x-ref fields (allows all of the updates in questions 02, 03, 04) to update comp code fields (comp code, number, to/from dates) and beneficiary phone number field
336	BUDS16	02	Maintain Bene MSP Occurrences	N No authority for this transaction Y Authority to maintain beneficiary MSP occurrences on BUDS/16
337				Reserved for future use
338				Reserved for future use
339	BUDS25	02	Update Crossover Records	N No authority for this transaction Y Authority to update crossover records on BUDS/25
340	BUDS26	02	Update Medigap	N No authority for this transaction Y Authority to update Medigap on BUDS/26
341	BUDS26	03	Add Medigap	N No authority for this transaction Y Authority to add Medigap on BUDS/26
342	BUDS26	04	Delete Medigap	N No authority for this transaction Y Authority to delete Medigap on BUDS/26
343	BUDS26	05	Update MSP	N No authority for this transaction Y Authority to update MSP on BUDS/26
344	BUDS26	06	Add MSP	N No authority for this transaction Y Authority to add MSP to BUDS/26
345	BUDS26	07	Delete MSP	N No authority for this transaction Y Authority to delete MSP from BUDS/26
346	COIN1	02	Update Coin Header	N No authority for this transaction Y Authority to update Complementary Insurance Header records
347	COIN1	03	Add Coin Header	N No authority for this transaction Y Authority to add Complementary Insurance Header records
348	COIN1	04	Delete Coin Header	N No authority for this transaction Y Authority to delete Complementary Insurance Header records
349				Reserved for future use
350	HARP	02	Update HCPCS	N No authority for this transaction Y Authority to update HCPCS
351	HARP	03	Add HCPCS	N No authority for this transaction Y Authority to add HCPCS
352	HARP	04	Delete HCPCS	N No authority for this transaction Y Authority to delete HCPCS
353	ICOR	02	Update DOD Field	N No authority for this transaction Y Authority to update the ICOR DOD field

Security Switch Values Sorted by Switch Number				
354	ICOR	03	Update DOR Field	N No authority for this transaction Y Authority to update the ICOR DOR field
355	ICOR	04	Maintain Outgoing Letter Screen	N No authority for this transaction Y Authority to maintain the ICOR Outgoing Letter screen
356	ICOR	05	Access to Other Operator Stats	N No authority for this transaction Y Authority to access other operators' ICOR statistics
357	ICOR	06	Delete ICOR Case	N No authority for this transaction Y Authority to delete an ICOR case
358	ICOR	07	Update/Delete Within ICOR	N No authority for this transaction Y Authority to update and delete within ICOR
359	ICOR	08	Add Within ICOR	N No authority for this transaction Y Authority to add within ICOR
360				Reserved for future use
361	ICOR	10	Update Request Case Count Field	N No authority for this transaction Y Authority to update the ICOR Request Case Count field
362	OLDE	02	Supervisor	N No authority for this transaction Y Authority for supervisor/administrator access to OLDE
363	VMAP4	16	Update CMN Status Table	N No authority for this transaction Y Authority to update the VMAP/4 CMN Status table
364	VMAP4	22	Maintain PIMR Edit Code Table	N No authority for this transaction Y Authority to maintain the VMAP/4 PIMR Edit Code Table
365	VMAP4	23	Maintain Claim Path Ownership	N No authority for this transaction Y Authority to maintain VMAP/4 claim path ownership
366	VMAP/4	24	Maintain VMAP 4C Error Handler Tables 0-9	N No authority for this transaction Y Authority to maintain VMAP/4C Error Handler tables 0–9
367	VMAP/4	25	Update MPFSDB Pricing Periods Table	N No authority for this transaction Y Authority to update VMSP/4C MPFSDB Pricing Periods Table
368	VMAP/4	26	Delete Accounting Status Codes	N No authority for this transaction Y Authority to delete Accounting Status Codes
369	VMAP4	27	Update VMAP/4C LMRP/NCD Code Description Table	N No authority for this transaction Y Authority to update the LMRP/NCD codes and descriptions
370	LTRO	02	Maintain LTRO Messages	N No authority for this transaction Y Authority to maintain LTRO messages
371	VMAP4	17	Update State Table	N No authority for this transaction Y Authority to update the VMAP/4 State table

Security Switch Values Sorted by Switch Number				
372	VMAP4	18	Update MSA Pricing Period Table	N No authority for this transaction Y Authority to update the VMAP/4 MSA Pricing Period table
373				Reserved for future use
374				Reserved for future use
375				Reserved for future use
376				Reserved for future use
377				Reserved for future use
378	MGTP	02	Maintain Biller Record	N No authority for this transaction Y Authority to maintain biller records
379	MGTP	03	Update ERN EFF DT field	N No authority for this transaction Y Authority to update ERN EFF DT field
380				Reserved for future use
381				Reserved for future use
382	MONI	02	Update Receivable Record	N No authority for this transaction Y Authority to update MONI receivable records
383	MONI	03	Add Receivable Record	N No authority for this transaction Y Authority to add MONI receivable records
384	MONI	04	Delete Receivable Record	N No authority for this transaction Y Authority to delete MONI receivable records
385	MONI	28	Authority for this Transaction	N No authority for this transaction Y Authority to update the status of a RAC receivable
386				Reserved for future use
387				Reserved for future use
388				Reserved for future use
389				Reserved for future use
390	MONIB	02	Update Misc/MAN Check Remark Field for Withholding Disbursements	N No authority for this transaction Y Authority to update the MONI Check Reconciliation Misc/Man Check Remark field for withholding disbursements
391				Reserved for future use
392	MONIB	03	Update Misc Check Withhold % Field	N No authority for this transaction Y Authority to update the MONI Check Reconciliation Misc Check Withhold % field
393	MONIB	04	Update Misc Check All Other Fields	N No authority for this transaction Y Authority to update all other MONI Check Reconciliation Misc Check fields
394	MONIB	05	Add Misc Check ICN Required	N No authority for this transaction Y Authority to add the required Misc. Check ICN field

Security Switch Values Sorted by Switch Number				
395	MONIB	06	Add Misc Check Remark Field	N No authority for this transaction Y Authority to add the Misc. Check Remark field
396	MONIB	07	Add Misc Check Withhold % Field	N No authority for this transaction Y Authority to add the Misc. Check Withhold % field
397	MONIB	08	Add Misc Check All Other Fields	N No authority for this transaction Y Authority to add all other Misc. Check Withhold fields
398	MONIB	09	Delete Misc Check	N No authority for this transaction Y Authority to delete Misc. Checks
399	MONIB	17	Update CC Request Field	N No authority for this transaction Y Authority to update the CC Request field
400				Reserved for future use
401	MONIB	10	Update MAN Check Withhold % Field	N No authority for this transaction Y Authority to update the Manual Check Withhold % field
402	MONIB	11	Update MAN Check all Other Fields	N No authority for this transaction Y Authority to update all other Manual Check Remark fields
403	MONIB	12	Add MAN Check ICN Required	N No authority for this transaction Y Authority to add the required Manual Check ICN fields
404				Reserved for future use
405	MONIB	13	Add MAN Check Withhold % Field	N No authority for this transaction Y Authority to add the Manual Check Withhold % field
406	MONIB	14	Add MAN Check All Other Fields	N No authority for this transaction Y Authority to add all other Manual Check fields
407	MONIB	15	Delete MAN Check	N No authority for this transaction Y Authority to delete Manual Checks
408	MONIB	16	Update Check Detail Remark Field	N No authority for this transaction Y Authority to update the Check Detail Remark field
409	MONIB	18	Update Check Detail Replace Check # Field	N No authority for this transaction Y Authority to update the Check Detail Remark field and replace the Check # field
410	MONIB	19	Update Check Detail All Other Fields	N No authority for this transaction Y Authority to update all other Check Detail fields
411	MONIB	20	Update Bank Error without Delete Authority	N No authority for this transaction Y Authority to update the Bank Paid Error Correction screen
412	MONIB	21	Update Bank Error with Delete Authority	N No authority for this transaction Y Authority to update and delete Bank Paid Error Correction records

Security Switch Values Sorted by Switch Number				
413	MONIB	22	Update Other Payee without Delete Authority	N No authority for this transaction Y Authority to update the Other Payee History screen
414	MONIB	23	Add Other Payee	N No authority for this transaction Y Authority to add Other Payee History
415	MONIB	24	Update Other Payee with Delete Authority	N No authority for this transaction Y Authority to update and delete Other Payee History
416	MONIB	25	Update Withholding	N No authority for this transaction Y Authority to update the Withholding Summary screen
417				Reserved for future use
418				Reserved for future use
419				Reserved for future use
420				Reserved for future use
421				Reserved for future use
422				Reserved for future use
423				Reserved for future use
424				Reserved for future use
425	MONIK		Add/Update Check Type, Check Status, and Check Reason fields	N No authority for this transaction Y Authority to add/update Check Type, Check Status, and Check Reason fields
426	MONIK		Add/Update all updateable fields other than Check Type, Check Status, and Check Reason	N No authority for this transaction Y Authority to add/update all updateable fields other than Check Type, Check Status, and Check Reason
427	MONIK	02	Update Checklog Record	N No authority for this transaction Y Authority to update MONI Check Log records
428	MONIK	03	Add Checklog Record	N No authority for this transaction Y Authority to add MONI Check Log records
429	MONIK	04	Delete Checklog Record	N No authority for this transaction Y Authority to delete MONI Check Log records
430	OLDS	02	Supervisor	N No authority for this transaction Y Authority for supervisor/administrator access to OLDS
431	PENS	02	Add/Update PENS Records	MedB only N No authority for this transaction Y Authority to add/update PENS records Note: This switch only applies in test mode.
432	VMAP2	03	Maintain QA Selection Card	N No authority for this transaction Y Authorization to maintain the QA Selection Card

Security Switch Values Sorted by Switch Number				
433	PENS	03	Delete PENS Records	MedB only N No authority for this transaction Y Authority to delete PENS records Note: This switch only applies in test mode.
434	PENS	04	Request PENS Report	N No authority for this transaction Y Authority to request PENS reports
435	PINQ	02	Provider Security Check	N No authority for this transaction Y Authority to access the Provider Security Check
436	STAT	02	Inquire on Other Operator STATS	N No authority for this transaction Y Authority to access other operator's Terminal Operator Statistics
437				Reserved for future use
438	VCAP	02	Totals	N No authority for this transaction Y Authority for VCAP exception processing, individual operator statistics, totals, operator statistics on other people
439	VCAP	03	Reprocess	N No authority for this transaction Y Authority for VCAP exception processing, individual operator statistics
440	VCAP	04	STATS for Others	N No authority for this transaction Y Authority for VCAP exception processing, individual operator statistics, operator statistics on other people
441	VCAP	05	Access CMNs w/Status Y in VMAP/4D	N No authority for this transaction Y Authority to access CMNs that have a Y in their Security field on the VMAP/4D STATCMN table (restricted status)
442	VCHK1	02	Update Payee Records	Empire only N No authority for this transaction Y Authority to update payee records in the Checkmate system
443	VCHK2	02	Update Rules	Empire only N No authority for this transaction Y Authority to update Rules in the Checkmate system
444	VCHK3	02	Update Alert Records	Empire only N No authority for this transaction Y Authority to update the Alert records in the Checkmate system
445	VCHK4	02	Update PARMS Except Purge Date	Empire only N No authority for this transaction Y Authority to update all the parms except Purge Date in the Checkmate system

Security Switch Values Sorted by Switch Number				
446	VCHK4	03	Update Purge Date	Empire only N No authority for this transaction Y Authority to update the Purge Date parm in the Checkmate system
447	VDME	02	Prior Auth Field Update Authority	N No authority for this transaction Y Authority to update the Prior Authorization field
448	VDME	03	Update/Add CMNs	N No authority for this transaction Y Authority to update/add CMNs
449	VDME	04	Send CMN Add/UPD/Del to CWF (Super Post/Super Delete)	N No authority for this transaction Y Authority to send add/update/ delete CMNs to CWF
450	VDME	05	QUES# 4 + UPD Init Date, Med Nec Length, HCPCS on Status 01CMNs	N No authority for this transaction Y Authority to send add/update/ delete CMNs to CWF and to update Init Date Med Nec Length, and HCPCS on Status 01 CMNs
451	VDME	06	QUES# 5 + UPD End Date on Capped Rental Revisions	N No authority for this transaction Y Authority to send add/update/ delete CMNs to CWF; to update Init Date Med Nec Length, and HCPCS on Status 01 CMNs; and to update the End Date on Capped Rental Revisions
452	VDME	07	UPD HICN, XREF1 and XREF2 on CMN	N No authority for this transaction Y Authority to update the HICN, XREF1, and XREF2 fields on CMNs
453				Reserved for future use
454	VDME	09	Update Fee Schedule Amount For IRP Items	N No authority for this transaction Y Authority to update the FEE SCHEDULE AMT field on IRP CMNs
455	VDME	10	Update Grid Edit Code	N No authority for this transaction Y Authority to update the Grid Edit Code on CMNs
456				Reserved for future use
457				Reserved for future use
458				Reserved for future use
459				Reserved for future use
460				Reserved for future use
461				Reserved for future use
462				Reserved for future use
463				Reserved for future use
464				Reserved for future use
465	VEC9	02	Update EC9 Records	N No authority for this transaction Y Authority to update Entry Code Nine records
466	VMAP4	19	Maintain Group CMN Table	N No authority for this transaction Y Authority to maintain the VMAP/4 Group CMN table

Security Switch Values Sorted by Switch Number				
467	VMAP1	02	Update VMAP/1.1	N No authority for this transaction Y Authority to update VMAP/1.1 (Name and Address / Control Options / Area Profiles)
468	VMAP1	03	Update VMAP/1.2	N No authority for this transaction Y Authority to update VMAP/1.2 (Automated Development Options)
469	VMAP1	04	Update VMAP/1.3	N No authority for this transaction Y Authority to update VMAP/1.3 (Interest Rates)
470	VMAP1	05	Update VMAP/1.4	N No authority for this transaction Y Authority to update VMAP/1.4 (Accounting Contractor Options)
471	VMAP1	06	Update VMAP/1.5	N No authority for this transaction Y Authority to update VMAP/1.5 (Accounting Interest Rates)
472	VMAP1	07	Update VMAP/1.6	N No authority for this transaction Y Authority to update VMAP/1.6 (HPSA Excessive Payment Report Request)
473	VMAP2	02	Add CWF History Request	N No authority for this transaction Y Authority to add CWF History Requests
474	VMAP3	02	Update Location Description	N No authority for this transaction Y Authority to update Location Descriptions
475	VMAP4	02	Update VMAP/4 Claim Parameters	N No authority for this transaction Y Authority to update VMAP/4C Claim Parameters except for: VMAP/4C Claim Path – see switch 365 VMAP/4C PIMR Edit Code – see switch 364 VMAP/4C Error Tables 0–9 – see switch 366 VMAP/4C MPFSDB Pricing Periods Table – see switch 367 VMAP/4C SPOT – see switch 480 VMAP/4C EMC/FASF – see switch 479 VMAP/4C Environ – see switch 478
476	VMAP4	03	Update VMAP/4 Accting Parameters	N No authority for this transaction Y Authority to update VMAP/4A Accounting Parameters
477	VMAP4	04	Update VMAP/4 MSN Parameters	N No authority for this transaction Y Authority to update VMAP/4 MSN Parameters
478	VMAP4	05	Update VMAP/4C ENVIRON and CONTACT tables and VMAP/4A HOLIDAY table	N No authority for this transaction Y Authority to update VMAP/4 Carrier Environment and Contact tables
479	VMAP4	06	Update VMAP/4C EMCEDITS, FASFEDIT and CARRIER Tables	N No authority for this transaction Y Authority to update VMAP/4 EMC and FASF tables

Security Switch Values Sorted by Switch Number				
480	VMAP4	07	Update VMAP/4 SPOT Table	N No authority for this transaction Y Authority to update VMAP/4 SPOT table
481	VMAP4	08	Update VMAP/4 Correspondence Parms	N No authority for this transaction Y Authority to update VMAP/4B Correspondence Parameters
482	VMAP4	09	Update VMAP/4 Alert Code Table	N No authority for this transaction Y Authority to update VMAP/4 Alert Code table
483	VMAP4	10	Maintain VMAP/4 DMERC Specialty Table	N No authority for this transaction Y Authority to maintain the VMAP/4D DMERC Specialty Table
484	VMAP4	11	Update VMAP/4A Banking Table	N No authority for this transaction Y Authority to update VMAP/4A Banking table
485	VMAP4	12	Inquiry into VMAP/4D Autocopy	N No authority for this transaction Y Inquire into VMAP/4D Autocopy
486	VMAP4	13	Add, Update, or Copy VMAP/4D Autocopy Options	N No authority for this transaction Y Authority to add, update, or copy in VMAP/4D Autocopy
487	VMAP4	14	Delete VMAP/4D Autocopy Options	N No authority for this transaction Y Authority to delete in VMAP/4D Autocopy
488	VANSCL	02	Update Retention Indicator	N No authority for this transaction Y Authority to update the VANS claims data retention indicator
489	VANSPE	02	Maintain Parameter Records	N No authority for this transaction Y Authority to maintain all VANS parameter records
490				Reserved for future use
491				Reserved for future use
492				Reserved for future use
493				Reserved for future use
494				Reserved for future use
495				Reserved for future use
496				Reserved for future use
497				Reserved for future use
498				Reserved for future use
499				Reserved for future use
500	VMAP5	02	Maintain Rebundling Tables	N No authority for this transaction Y Authority to maintain the VMAP/5 Rebundling tables
501				Reserved for future use
502				Reserved for future use
503	VMAP1	08	Update VMAP/1.7	N No authority for this transaction Y Authority to update VMAP/1.7 (Deductibles and Limits)
504				Reserved for future use

Security Switch Values Sorted by Switch Number				
505				Reserved for future use
506	VMAP6	02	Update VMAP/6	N No authority for this transaction Y Authority to update VMAP/6 (Pre-Payment Utilization Options)
507				Reserved for future use
508				Reserved for future use
509				Reserved for future use
510				Reserved for future use
511				Reserved for future use
512				Reserved for future use
513				Reserved for future use
514				Reserved for future use
515				Reserved for future use
516				Reserved for future use
517	VMAP7	02	Update VMAP/7.1,7.3,7.5 and 7.6	N No authority for this transaction Y Authority to update VMAP/7.1, 7.3, 7.5, and 7.6 (Claim History Reporting Sub-System)
518	VMAP7	03	Access to HCFA Initiated Reports (7.2)	N No authority for this transaction Y Authority to access VMAP/7 HCFA Initiated Reports (7.2)
519	VMAP7	04	Access to PIMB Universe Request (7.4)	N No authority for this transaction Y Authority to access VMAP/7 PIMB Universe Request (7.4)
520				Reserved for future use
521				Reserved for future use
522				Reserved for future use
523				Reserved for future use
524	VMON	02	Full Claims Operator	N No authority for this transaction Y Authority to access VMON as a full claims operator
525	VMON	03	Suspense Claims Operator	N No authority for this transaction Y Authority to access VMON as a suspense claims operator
526	VMON	04	Adjustment Claims Operator	N No authority for this transaction Y Authority to access VMON as an adjustment claims operator
527	VMON	21	LMRP/NCD Numbers	N No authority for this transaction Y Authority to use LMRP/NCD Numbers
528	VMON	22	Update CWF Override Group F	N No authority for this transaction Y Authority to update CWF Override Group F (7282)
529	VMON	05	EMC Operator for Sequential Terms	N No authority for this transaction Y Authority to access VMON as an EMC (Electronic Media Claims) operator for sequential terminals

Security Switch Values Sorted by Switch Number				
530	VMON	06	Force Codes 3, 5, L, R, T, Y	N No authority for this transaction Y Authority to use Claim Force Codes 3, 5, L, R, T, and Y
531	VMON	07	Force Codes N, V, Z	N No authority for this transaction Y Authority to use Claim Force Codes N, V, and Z
532	VMON	08	Quality Review Operator	N No authority for this transaction Y Authority to access VMON as a Quality Review operator
533	VMON	09	QCN Grab Authority	N No authority for this transaction Y Authority to take a PEN CMN from the CMN List Screen and put it on the line of a claim
534	VMON	10	Force Codes 1 and 2 Authority	N No authority for this transaction Y Authority to use Claim Force Code 1 to bypass edit 0192-NO CHK/NO ADJST and Claim Force Code 2 to bypass combined edits 0192-NO CHK/NO ADJST and 1085-PAST FILE LIMIT when adjusting claims
535	VMON	11	Update CWF Override Group A	N No authority for this transaction Y Authority to update CWF Override Group A (5232, 524Z, 525Z, 538Q, 538Z, 5389, 5390, 5514, 7253, 7257, 7258, 7259, 7260, 7261, 7269, 7275, 7290)
536				Reserved for future use
537				Reserved for future use
538				Reserved for future use
539				Reserved for future use
540				Reserved for future use
541	VNOT	02	Update Notepad Records	N No authority for this transaction Y Authority to update Notepad records
542	VNOT	03	Add Notepad Records	N No authority for this transaction Y Authority to add Notepad records
543	VNOT	04	Delete Notepad Records	N No authority for this transaction Y Authority to delete Notepad records
544	VNOT	05	Maintain Bene Medical notes	N No authority for this transaction Y Authority to maintain Bene Medical notes
545				Reserved for future use
546				Reserved for future use
547				Reserved for future use
548	VSAF	02	Request Reports	N No authority for this transaction Y Authority to request SAFE reports
549	VSAF	03	View Security File Changes	N No authority for this transaction Y Authority to view Security File changes

Security Switch Values Sorted by Switch Number				
550	VSAF	04	Maintain System/Prod Crtl Screen	N No authority for this transaction Y Authority to maintain the SAFE System/Prod Crtl screen
551	VMAP2	04	Add Purge History Request	N No authority for this transaction Y Authority to add Purge History Requests
552	XADJ	02	Update VAR1/VAR2 Fields on Define Batch Screen for own UserID	N No authority for this transaction Y Authority to update the VAR1/VAR2 field on the Define Batch Screen for your own User ID
553	XADJ	03	Full Maintenance of Define Batch Screen for Own UserID	N No authority for this transaction Y Authority for full maintenance to the Define Batch Screen for your own User ID
554	XADJ	04	Full Maintenance of Define Batch Screen for All UserIDs	N No authority for this transaction Y Authority for full maintenance to the Define Batch Screen for all User IDs
555	XADJ	05	Update Process and Select Limits Fields on Define Batch Screen	N No authority for this transaction Y Authority to update the Process and Select Limits fields on the Define Batch Screen
556	SUPR	02	Maintain XMOD, XADJ Events	N No authority for this transaction Y Authority to maintain XMOD and XADJ SuperOp Events
557	SUPR	03	Maintain VOQC Events	N No authority for this transaction Y Authority to maintain VOQC SuperOp Events
558	SUPR	05	Maintain all other Events	N No authority for this transaction Y Authority to maintain all other SuperOp Events
559	SUPR	06	Question # 2 plus Delete XMOD, XADJ Events	N No authority for this transaction Y Authority to maintain XMOD and XADJ SuperOp Events; can also delete XMOD and XADJ Events
560	SUPR	07	Question # 3 plus Delete VOQC Events	N No authority for this transaction Y Authority to update SuperOp VOQC Events and delete VOQC SuperOp Events
561	SUPR	09	Question # 5 plus Delete all other Events	N No authority for this transaction Y Authority to maintain all other SuperOp Events; also can delete all other Events
562	SUPR	10	Question # 6 plus Change Status to Production for XMOD, XADJ Events	N No authority for this transaction Y Access SuperOp as a super reviewer; allows the operator to maintain XMOD and XADJ Events; to delete XMOD and XADJ Events; and to change the status of XMOD and XADJ Events to Production

Security Switch Values Sorted by Switch Number					
563	SUPR	11	Question # 7 plus Change Status to Production for VOQC Events	N Y	No authority for this transaction Authority to maintain VOQC SuperOp Events, to delete VOQC SuperOp Events, and to change the status of VOQC Events to Production
564	SUPR	13	Question # 9 plus Change Status to Production for all other Events	N Y	No authority for this transaction Authority to maintain all other Events, to delete all other Events, and to change the status of all other Events to Production
565	SUPR	14	Question # 10 plus Archive XMOD,XADJ Events	N Y	No authority for this transaction Access SuperOp as a super reviewer; allows the operator to maintain XMOD and XADJ Events; to delete XMOD and XADJ Events; to change the status of XMOD and XADJ Events to Production; and to archive XMOD and XADJ Events
566	SUPR	15	Question # 11 plus Archive VOQC Events	N Y	No authority for this transaction Authority to update SuperOp VOQC Events, to delete VOQC Events, to change the status of VOQC Events to Production, and to archive VOQC Events
567	VMAP4	20	Update Form/Version Table	N Y	No authority for this transaction Authority to update the VMAP/4 Form/Version table
568	VMAP4	21	Update CMN Related Table	N Y	No authority for this transaction Authority to update the VMAP/4 CMN Related table
569	SUPR	17	Question # 13 plus Archive All other Events	N Y	No authority for this transaction Authority to maintain all other SuperOp Events, to delete all other Events, to change the status of all other Events to Production, and to archive all other Events
570	SUPR	04	Maintain SURE Events	N Y	No authority for this transaction Authority to maintain SURE Events
571	SUPR	08	Question # 4 plus Delete SURE Events	N Y	No authority for this transaction Authority to maintain SURE Events and authority to delete SURE Events
572	SUPR	12	Question #8 plus Change Status to Production for SURE Events	N Y	No authority for this transaction Authority to maintain SURE Events, to delete SURE Events, and to change the status of SURE Events to production
573	SUPR	16	Question # 12 plus Archive SURE Events	N Y	No authority for this transaction Authority to maintain and delete SURE Events, to change the status of SURE Events to production, and to archive SURE Events

Security Switch Values Sorted by Switch Number				
574	XLST	02	Select/Unselect/Adjust Unsolicited Type U Claims	N No authority for this transaction Y Authority to select, unselect, and adjust type U unsolicited claims
575	SUPR	18	Savings Inquiry Only	N No authority for this transaction Y Authority to create an inquiry or view the Event Category Savings Statistics and Event Savings Statistics List screens.
576	SUPR	19	Savings Update for Event Categories	N No authority for this transaction Y Authority to update the Event Category Assignment/Definition screen. Note: There is no inquiry authority for the Event Category Assignment/Definition and the Event Category Salary Information screens.
577	SUPR	20	Question # 18 and 19 for Savings	N No authority for this transaction Y Authority to view the Event Category Savings Statistics and Event Savings Statistics List screens and update the Event Category Assignment/Definition screen for Savings. Note: There is no inquiry authority for the Event Category Assignment/Definition and the Event Category Salary Information screens.
578	SUPR	21	Question #18 and 19 plus Category and Salary	N No authority for this transaction Y Authority to view the Event Category Savings Statistics and Event Savings Statistics List screens; update the Event Category Assignment/Definition screen for Savings, plus update Event Category Salary Information screens. Note: There is no inquiry authority for the Event Category Assignment/Definition and the Event Category Salary Information screens.
579	SUPR	22	Can View Table Data?	N No authority for this transaction Y Authority to view table data
580	SUPR	23	Can Update Table Data?	N No authority for this transaction Y Authority to update table data
581	SUPR	24	Can Define Tables?	N No authority for this transaction Y Authority to define tables
582	SUPR	25	Can Drop Tables?	N No authority for this transaction Y Authority to drop tables
583	XLST	03	Process Bene/Prov=0 Batches?	N No authority for this transaction Y Authority to process BENE/PROV = O batches in XLST
584	XADJ	06	Create Bene/Prov=0 Batches?	N No authority for this transaction Y Authority to create BENE/PROV = O batches on the Define Batches screen

Security Switch Values Sorted by Switch Number				
585	VSAF	05	Invoke SAFE Pop-Up in ViPS Test?	N No authority for this transaction Y ViPS only – authority to invoke the SAFE pop-up
586	XLST	04	Select/Unselect/Adjust Type M Unsolicited Claims	N No authority for this transaction Y Authority to select/unselect/adjust type M unsolicited claims

APPENDIX F - GUIDANCE FOR GENERATING SECURITY REPORTS

FISS

Operator Control File (FSSOPER)

- Select File Maintenance Menu
- Transaction #57
- Transcation Type I (Inquiry)
- Press Enter

Figure 11 Operator Control File Example

```
    OPER                                        MEDICARE A                                                    DATE:
                                              OPERATOR CONTROL
0 OPERATOR ID: A123          PASSWORD:        DEPARTMENT: 555      ACCESS:  N
  FIRST NAME: JOHN               LAST NAME: DOE                    PLAN:  1  OP:
                                                                              DT:  010108
0 S-L EXCLUSION:
  S-L INCLUSION:
0                                              TRANSACTION SECURITY
  FUNCTION              ACCESS                FUNCTION              ACCESS                FUNCTION              ACCESS
  *-------------------------------------------------------------------------------------------------------------------
0 ACS SYSTEM              N                   ADJ REASON CODE         I                   BATCH HEADER            N
  BATCH SUM-DETAIL        Y                   BENEFICIARY             I                   HOME HEALTH RAP         N
  CLAIMS                  Y                   CLAIM AUDIT             N                   CLAIM SUMMARY           I
  CWF ATTACH              I                   EXIT FLAG               N                   EMC                     N
  ERRS RET TO PRO         N                   ESRD PARAMETER          I                   ESRD LAB                N
  ESRD REMARKS            I                   ESRD SUM HISTORY        N                   HCPC                    I
  ICD9 CODES              I                   LIMITATION-LIAB         N                   MED POLICY              I
  MSP                     I                   MSP SAVINGS             I                   OPERATOR CONTROL        N
  PACEMAKER               N                   PAYMENT-INTEREST        N                   PENDING PRO ADJ         N
  PHYSICIAN               I                   POST PAY                Y                   PPS                     I
  PRO ADJ ERR CODES       I                   PROVIDER                I                   PROVIDER ADDR           I
  REASON CODES            I                   RET TO PRO ADDR         N                   REVENUE CODES           N
  STATUS LOCATION         N                   POST PAY ACTION         Y                   BENE-REMARKS            I
  EXT BENE INQUIRY        N                   EXT CLAIMS              N                   DRG PRICER              I
  EXT ICD9 INQUIRY        N                   EXT HCPCS INQ           N                   EXT REV CODE INQ        N
  EXT PACEMAKER           N                   AMBULANCE               N                   HOME HEALTH             N
  THERAPY                 I                   ONLINE REPORTS          I                   OTHER FUNCTIONS         N
  DME HISTORY             N                   EXT ADJ REASONS         N                   PLAN CARE SELECT        N
  EXT REASON CODES        N                   EXT ADJUSTMENTS         N                   COB PARTNERS            N
  FSSA CONTROL            N                   CWF XMIT LOCS           N                   INTERMEDIARY REC        I
  CARRIER RECORD          N                   SITE CONTROL            N                   1ST CLAIM DEVEL         N
  REPORT DEFAULTS         N                   R308 PRIOR PEND         N                   RPT FILE TO READ        N
  PURGE-RETRIEVE          N                   RTS LETTERS             N                   RTS TRACKING            N
  RTS INSURER             N                   RTS SYSTEM CNTL         N                   RTS SPECIAL REQ         N
  INHOUSE SECURITY        N                   DDE SECURITY            N                   EXT ESRD HCFA382        N
  ANSI CODES              I                   ONLINE RPT CNTL         N                   EXT DME HISTORY         N
  MSN MESSAGES            I                   FDA IDE DEVICES         N                   MEDICARE CHOICES        N
  EXT CHK HISTORY         N                   UNDELIV MAIL            N                   ESRD ATTACH             N
  CTR OF EXCELLENCE       N                   OUTPATIENT PPS          N                   EDI ENROLLMENT          N
1    OPER                                        MEDICARE A                                                    DATE:
                                              OPERATOR CONTROL
0 OPERATOR ID: A123          PASSWORD:        DEPARTMENT: 555      ACCESS:  N
0                                          FINANCIAL SECURITY TRANSACTIONS
  FUNCTION              ACCESS      FUNCTION              ACCESS      FUNCTION              ACCESS      FUNCTION              ACCESS
  *-------------------------------------------------------------------------------------------------------------------
0 FINANCIAL MASTER        N         CASH DISBURSEMENTS      N         ACCELERATED W-HOLDING   N         INTERMED CYCLE          N
  OTHER PAY               N         HCFA 456                N         MANUAL CHECKS           N         INTERMED BANK HOLIDAYS  N
  BENE RECONCILIATION     N         HCFA 1521               N         MANUAL VOIDS            N         INTERMEDIARY-ADD        N
  PAYMENT                 N         HCFA 1522               N         MANUAL STOPS            N         SETTLE OVERPAY RATE     N
  SETTLEMENT              N         HCFA IBPR REPORT        N         CHECK TYPE CODES        N         GRH PERCENT             N
  WITHHOLDINGS            N         PENALTY RELEASE         N         CHECK HISTORY           N         GRH RELEASE             N
  MANUAL CHECK PROCESS    N         REFUND                  N         PAYEE HISTORY           N         ELECTRONIC FUND DELAY   N
  CHECKS                  N         ACCELERATED PAYMENT     N         BANK PAID ERROR         N         GENERAL LEDGER MAINT    N
  REMITTANCE              N         SETTLEMENT (ADD)        N         ADVISE SUMMARY          N         GENERAL LEDGER BALANCE  N
  ACCOUNTS PAYABLE        N         SETTLEMENT CASH RECOUP  N         PRIMARY REMIT SORT      N         COST REPORT CNTL LOG    N
  ELECTRONIC FUNDS        N         SETTLEMENT ACCTS REC    N         SECONDARY REMIT SORT    N
  SYSTEM PROFILE          N         SETTLEMENT ADJUSTMENTS  N         ACCOUNTS PAY DETAIL     N
  INTERMEDIARY ADMIN      N         PROVIDER STATEMENTS     N         ACCOUNTS PAY REFUND     N
  SYSTEM ADMIN            N         SETTLEMENT INQUIRY      N         ELECT FUNDS TRANSFER    N
  CHART OF ACCOUNTS       N         PENALTY .               N         ELECT FUNDS-ADJUST      N
  CASH RECEIPTS           N         CLAIM ACCOUNTS REC      N         DATA PURGE PROFILE      N
  BENE RECONCILIATION     N         SETTLEMENT              N         INTERMED ADMIN DATA     N
-                                      AUTHORIZED REASON CODE OVERRIDES
  REASON AUTH  REASON AUTH  REASON AUTH  REASON AUTH  REASON AUTH  REASON AUTH  REASON AUTH  REASON AUTH  REASON AUTH  REASON AUTH
   CODE   SW    CODE   SW    CODE   SW    CODE   SW    CODE   SW    CODE   SW    CODE   SW    CODE   SW    CODE   SW    CODE   SW
```

Note: This is only one example of an Operator Control File. Format of the report may vary by Medicare Contractor.

MCS: Clerk File Security Report (H99CRCF)
Job Number: D457
DD: DD3
Module: H99PCSEC
Proc Step: PS1080

Figure 12 Clerk File Security Report (H99CRCF)

```
 REPORT ID: H99RCRCF                        MCS QUALITY ASSURANCE                          FEBRUARY 07, 2005          PAGE:   1
                                            CLERK FILE SECURITY REPORT
                                                                                1 1 1 1 1  1    1111222222222233 3 33333334444444444555555
  1      2                                  3   4  5     6          7    8 9    0 1 2 3 4  5    6789012345678901 2 34567890123456789012345
 CLRK CLERK NAME                          DEPT D  U LAST UPDATED NICKNAM S B-D  H S S S S LIMIT AACDGHILMMSSTCVL H AAAAAAEEECCCCHACCCDEEHE
 ID   FIRST/LAST                              I  N   DATE/BY            C   A  O T T T T       GULETESCSSMSRAHC M CCCCCC1231234RDERWIDDDO
                                              V  I                      F   T  L 1 2 3 4       EDRO L EGPR N    R SSSSSS        SNIFAIAEM
                                                 T                          E  D                 IKL P F RT G    S 123456         ST GTUAB

                                             55556 666666 666      77777777788888888889 99999999 9  1  1  1 1 1 1 1 1 1 1 1 11 1
                                             67890 123456 789      01234567890123456789 12345678 9  0  0  0 0 0 0 0 0 0 0 11 1
                                                                                                   0  1  2 3 4 5 6 7 8 9 01 2
-                                            MNPPT MNSC2P SSS      IRNAIXXXAAAAFIBITTNRV MMSSSMAC * *2 *4 *9 J # W I R X O VP PSWD
                                             OACRA MUUO5S 123      AECFGABOASIPIRSPXCGGQ FTPTTDRT                           IR UPDT
                                             DRFOC     9U                                US                             OO
                                             IR CS     0P                                PP                             LD


AC0   ACLERK          AAAAACLERK      000 00 0 000000      AAAAA     N 0000 N X X X X 00000 NUNUUNINNNNIUNNI I UIIIIUUUUUUUUNNNNNNNNN
                                     NNNNN UUUUNN NNN      NUNUNNNNUIIIIIIUUUNUU NNNNNNN  Y Y  Y  Y  Y Y Y Y Y Y   NY 010140

BC0   BCLERK          BBBBBCLERK      000 00 0 000000      BBBBB     N 0000 N X X X X 00000 NUNUUNINNNNIUNNI I UIIIIUUUUUUUUNNNNNNNNN
                                     NNNNN UUUUNN NNN      NUNUNNNNUIIIIIIUUUNUU NNNNNNN  Y Y  Y  Y  Y Y Y Y Y Y   NY 010140

CC0   CCLERK          CCCCCCLERK      000 00 0 000000      CCCCC     N 0000 N X X X X 00000 NUNUUNINNNNIUNNI I UIIIIUUUUUUUUNNNNNNNNN
                                     NNNNN UUUUNN NNN      NUNUNNNNUIIIIIIUUUNUU NNNNNNN  Y Y  Y  Y  Y Y Y Y Y Y   NY 010140

                                                TOTAL NUMBER OF CLERKS =  113..
```

VMS: Operator Security List Report (SE5002)
Job: VIPSDSE1
Program: VMSSE550

Table 7 Operator Security List Report (SE5002)

CARRIER: CARR# CARRIER NAME RUN DATE: MM/DD/YY
PROGRAM: VMSSE550 MEDICARE PART B
RUN TIME: HH:MM:SS REPORT: SE5502 OPERATOR SECURITY LIST
PAGE: 1

REQUESTOR ID: 0000000 DATE/TIME: MM/DD/YY HH:MM:SS SWITCH NUMBER: 111

USER ID	OPID	NAME	ST	TYPE	JOB FUNC	DEPT	COMMENT
0000000	010	UNASSIGNED					
0000000	011	MARY-S	A	3		CARR	
0000000	012	UNASSIGNED	A	3		CARR	
0000000	013	JAMES-D	A	3		CARR	
0000000	014	UNASSIGNED	A	3		CARR	
0000000	015	PATRICIA-J	A	3		CARR	
0000000	016	UNASSIGNED	A	3		CARR	
0000000	017	UNASSIGNED	A	3		CARR	
0000000	018	UNASSIGNED	A	3		CARR	
0000000	019	BARBARA-J	A	3		CARR	
0000000	020	UNASSIGNED	A	3		CARR	
0000000	021	UNASSIGNED	A	3		CARR	
0000000	022	WILLIAM-M	A	3		CARR	
0000000	023	ELIZABETH	A	3		CARR	
0000000	024	UNASSIGNED	A	3		CARR	
0000000	025	UNASSIGNED	A	3		CARR	
0000000	026	UNASSIGNED	A	3		CARR	
0000000	027	UNASSIGNED	A	3		CARR	
0000000	028	UNASSIGNED	A	3		CARR	
0000000	029	UNASSIGNED	A	3		CARR	
0000000	030	LINDA-W	A	3		CARR	
0000000	031	UNASSIGNED	A	3		CARR	
0000000	032	ROBERT-W	A	3		CARR	
0000000	033	UNASSIGNED	A	3		CARR	
0000000	034	MICHAEL-T	A	3		CARR	
0000000	035	UNASSIGNED	A	3		CARR	
0000000	036	UNASSIGNED	A	3		CARR	
0000000	037	UNASSIGNED	A	3		CARR	
0000000	038	JOHN-M	A	3		CARR	
0000000	039	UNASSIGNED	A	3		CARR	
0000000	040	BARBARA-S	A	3		CARR	
0000000	041	UNASSIGNED	A	3		CARR	
0000000	042	UNASSIGNED	A	3		CARR	
0000000	043	LINDA-J	A	3		CARR	
0000000	044	UNASSIGNED	A	3		CARR	
0000000	045	UNASSIGNED	A	3		CARR	
0000000	046	PATRICIA	A	3		CARR	
0000000	047	UNASSIGNED	A	3		CARR	
0000000	048	JOHN-D	A	3		CARR	
0000000	049	UNASSIGNED	A	3		CARR	
0000000	050	UNASSIGNED	A	3		CARR	

VMS: Operator Security Detail Report (SE5501)
Job: VIPSDSE1
Program: VMSSE550

Figure 13 Operator Security Detail Report (SE5501)

```
CARRIER: CARR#                                          CARRIER NAME                                          RUN DATE: MM/DD/YY
PROGRAM: VMSSE550                                     MEDICARE PART B                                         RUN TIME: HH:MM:SS
REPORT:  SE5501                                     OPERATOR SECURITY DETAIL                                     PAGE:          1

 REQUESTOR ID: V000000    DATE/TIME:  MM/DD/YY   HH:MM:DD   SWITCH NUMBER: 999

                                                SECURITY INFORMATION

USER ID: 0000000     NAME: ELIZABETH JOHNSON                        STATUS:A

DEPT: CARR        JOB FUNCTION:                                         CARRIER: CARR#

OPER ID: 000         PROVIDER:                EAR IND:  NN                CONTRACTOR: 1
COMMENTS:


                                                SECURITY SWITCHES
          0                   1                   2                   3                   4                   5
--RANGE--  1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0
001 - 050  Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y N Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y
051 - 100  Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y N N N Y Y Y Y Y Y Y Y Y Y Y Y Y Y
101 - 150  Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N
151 - 200  Y Y Y Y Y Y Y Y N N N N Y N N N N N N N N N N N N N Y Y Y Y Y N N N N N N N Y Y Y Y N N Y Y Y N Y Y
201 - 250  Y Y Y Y N Y Y Y Y Y Y N N N Y Y Y Y Y Y N N N N N N N N N Y Y Y Y Y Y Y Y Y Y Y Y N Y Y Y Y Y Y Y
251 - 300  Y Y Y Y Y Y Y Y Y Y Y N N N N N N N N N N Y Y Y Y N N N N N N N N N N Y Y Y N N N N N N N Y N N N
301 - 350  N N N N N N N N Y N Y Y Y Y N N N N N Y Y Y N N N N N N N N Y Y Y Y N Y Y Y Y N Y Y Y Y Y Y Y Y Y
351 - 400  Y Y Y Y Y Y Y Y Y Y Y N N N N N N N N Y N N Y Y Y Y Y N N N Y Y Y N N N N N N N N Y N N N Y N N N
401 - 450  N Y N N N Y Y N N Y Y Y Y Y N N N N N N N N N N N N N Y Y Y N Y Y N N N Y Y N N N N N N N N N Y N N
451 - 500  N N N N N N N N N N N N N N N N Y Y Y Y Y Y Y Y Y Y Y Y N Y Y N N Y N N N N N N N N N N N N N N N Y
501 - 550  N N N N N N Y N N N N N N N N N Y N N N N N Y Y Y Y N N N N N N N N N Y Y Y Y N N N N N N N N N N
551 - 600  Y N N N N Y N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N
601 - 650  N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N
651 - 700  N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N
701 - 750  N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N
751 - 800  N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N
801 - 850  N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N
851 - 900  N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N
901 - 950  N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N
951 - 999  N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N N
```

Note: Medicare Contractors using the Job Function feature will find that the security switches in the Operator Security Detail Report show the value of an asterisk(*). Any switch settings which have deviated from the role/template will show as a Y or N value.

(This Page Intentionally Blank)