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

CMS Security Whitepaper:

Direct Access to Data Whitepaper

FINAL
Version 2.0
March 08, 2009

(This Page Intentionally Blank)

SUMMARY OF CHANGES IN *DIRECT ACCESS TO DATA WHITEPAPER*, VERSION 2.0

1) Converted baseline version dated January 22, 2007 to updated CMS style format.
2) Moved Section 1, Introduction, from before Table of Contents to after.
3) Removed former Appendix A CSRs and added pointer to new CMSRs.
4) Added titles to Figure 1 and 2 in Appendix C.
5) Added title to Figure 3 in Appendix D.
6) Removed Section 3.3 (TSS) and TSS term from Appendix B, Glossary.
7) Add MAC to contractors list in Section 1.0.
8) Added references to RACFRPT 3-5 and RACFRPT2 to Section 3.1 Step 5 and Step 6, respectively.
9) Added update and violation activity guidance to the 4th bullet in Section 5, Documentation Requirements.
10) Added additional guidance to Section 6, Conclusion.

SUMMARY OF CHANGES IN *DIRECT ACCESS TO DATA WHITEPAPER*, VERSION 1.0

1) Baseline Version 1.0.

(This Page Intentionally Blank)

TABLE OF CONTENTS

LIST OF FIGURES

(This Page Intentionally Blank)

1 INTRODUCTION

Direct access to Medicare data allows users to gain access and modify medical and financial information outside of application controls, introducing potential threats to the integrity and reliability of the data. In some cases direct data access may be required in order to perform job responsibilities. Through the implementation of change control processes, audit logging, and other controls; the likelihood of unauthorized or erroneous changes to Medicare data via direct access can be significantly limited and/or detected.

This whitepaper has been created to assist Medicare contractors in determining the appropriateness of controls over direct access to data. Topics presented within this document include the following:

- background of direct access to data;
- results of the direct data access review;
- instructions for the review of direct access to Medicare data for Fiscal Intermediaries, Carriers, or MACs using RACF, ACF2, or Top Secret mainframe security;
- roles of the Data Centers in implementing controls over direct data access; and
- documentation requirements.

This paper servers to provide a foundation for CMS management and business partners to ensure that key controls pertaining to direct access to Medicare data are fully incorporated into CMS' control environment.

In today's world, access to data is a routine and essential aspect of operating computer systems and applications. It is not likely that management can totally eliminate the risks associated with direct access to data or remove all direct access. Direct access to data is needed to review and modify errors in the data thereby ensuring the data's integrity. However, such access presents a direct threat to the integrity and reliability of the data if sufficient controls have not been designed and implemented to ensure all changes made via direct access are proper. Because direct access to data circumvents controls built into applications (edits, audit trails, reconciliations), changes made directly to the data are inherently more risky than changes made through applications.

Management should ensure an appropriate balance of controls exists to ensure there is no more than a remote likelihood that a material misstatement of the financial statements could arise from unauthorized or erroneous changes to Medicare data via direct data access. In previous audits, it was noted that contractors had excessive access to Medicare data residing at many of the data centers. During the Chief Financial Statement Act Audit of the CMS Financial Statements for FY 2006, an examination of access to production claims data maintained and processed at the data centers was performed. The examination consisted of the following procedures for each Fiscal Intermediary, Carrier, DMERC, and CWF host:

- Inspection of a decomposition of naming standards for the datasets housing Medicare related data;

- Determination of who had been granted access to the datasets;
- Identification of users with greater than READ access;
- Inspection of dataset audit settings; and
- Validation that all Medicare-related datasets had auditing enabled.

The audit noted that employees had been granted access directly to Medicare claims data that would allow them to update Medicare claims data without following normal change processes and controls. Additionally, it was noted that access was not being logged and monitored to prospectively review its use and propriety. The lack of controls over direct access to data could result in user access to production datasets that may have not been appropriate thereby increasing the likelihood of fraud or unauthorized changes to Medicare data without detection.

Fiscal Intermediaries, Carriers, DMERCs, MACs, and CWF hosts had not limited direct access above READ to Medicare production datasets to only those personnel who required direct access for their job function nor had they implemented processes for logging and monitoring direct access to production datasets.

Medicare contractors should evaluate the appropriateness and need for direct access to Medicare-related data. This should include an evaluation of the environment, an assessment of the risks associated with the direct data access, and an assessment of the controls presently in place.

There are many factors to consider when determining the appropriate use of direct access to Medicare data. These factors include, but are not limited to:

- Business purpose for direct access to data;
- Inherent risks of the data;
- Access assignments for individuals with direct access based on job responsibilities and management's approved intent;
- Restriction of access to only individuals responsible for legitimate IT maintenance activities and appropriate segregation of duties;
- Controls to periodically review data access rights to ensure they remain consistent with job responsibilities and management's approved intent;
- Supervision of those with data access rights;
- Controls to provide access only on a temporary, as needed basis;
- Controls to independently track and monitor the activities of those accessing data directly;
- Background checks or other controls to properly consider the integrity of individuals with sensitive access rights;
- Controls in place to ensure that individuals with direct access are informed, understand, and acknowledge that accessing or changing data files outside of the normal, documented procedures presents risks that may have serious consequences;

- A formal change management process to control all data changes, including changes made via direct data access, including formal approvals;
- Controls in place for the periodic review of all standing or accumulated data elements changed from one period to the next; and
- Other controls (manual or automated) to ensure data have not been changed other than as intended.

2 SUMMARY OF RESULTS OF DIRECT DATA ACCESS REVIEW

During the Chief Financial Statement Act Audit of the CMS Financial Statement for FY 2006, access to production claims data maintained and processed at the data centers for each of the thirty Fiscal Intermediaries and Carriers was tested. Testing revealed problems with direct access to data at ninety-three percent of the Fiscal Intermediaries and Carriers. Specifically, testing confirmed that:

- Eighty-seven percent of Fiscal Intermediaries had unmonitored direct access to Medicare datasets;
- Ninety-four percent of Carriers had unmonitored direct access to Medicare datasets;
- One hundred percent of DMERCs had unmonitored direct access to Medicare datasets; and
- One hundred percent of CWF hosts had unmonitored direct access to Medicare datasets.

Note that within MCS (Carriers), direct access was required for GDX datasets because access to these datasets is required to allow users to update SCF tables.

Overall, most Fiscal Intermediaries and Carriers were not reviewing direct access to data. In many cases the Fiscal Intermediaries and Carriers were not getting information from their respective data centers to allow performance of the review process. In cases where this information was provided, the individuals responsible for the review often lacked the technical knowledge to appropriately read and assess the reports.

3 INSTRUCTIONS FOR REVIEWING DIRECT ACCESS TO MEDICARE DATASETS

1.1 INSTRUCTIONS FOR FI, CARRIER, OR MAC USING RACF MAINFRAME SECURITY

Step 1

Identify all data files containing Medicare claims data. Document file names and their contents. This may involve having the data centers review Job Control Language (JCL) to identify the data files if strong, well known naming conventions are not in place for these files. Create a process to ensure update and maintenance of file names and their contents to ensure they remain current.

Step 2[1]

Create standardized reports to document persons granted access to update Medicare claims data files. In RACF, the Dataset Monitor (DSMON) produces a selected datasets report which lists all the datasets, including the RACF database or databases, that meet one or more of the selection criteria that the DSMON report uses. For each selected dataset, the report specifies the serial number of the volume on which the dataset resides, the selection criterion, whether the dataset is RACF-indicated or RACF-protected, and the universal access authority (UACC) for the dataset. If a dataset or RACF database meets more than one selection criterion, there is a separate entry for each criterion. You can use the selected datasets report to determine which system and RACF datasets are protected by RACF and which are not. You can also check to learn whether the UACC associated with each of the datasets is compatible with the resource access control requirements of your installation.

Column Headings of the report are as follows:

- **DATASET NAME**: Name of the dataset.
- **VOLUME SERIAL**: Is the serial number of the direct access volume on which the dataset resides. If the dataset is not cataloged, this column is blank.
- **SELECTION CRITERION**: Is the criterion that was used to select the dataset for the report. The following entries may appear:
- **RACF INDICATED**: Indicates whether the dataset is RACF-indicated. The following entries may appear:
  - **YES**: Indicates that the RACF indicator for the dataset is on.
  - **NO**: Indicates that the RACF indicator for the dataset is off.

[1] Information from this section obtained from pages 108-109 of the z/OS Security Server RACF Auditor's Guide, V1R6.0.

  - **N.C.**: **I**ndicates that the dataset is not listed (cataloged) in the master catalog.
  - **N.M.**: **I**ndicates that the DASD volume on which the dataset resides is not mounted or has been dynamically deleted.
  - **N.F.**: **I**ndicates DSMON cannot find the dataset on the specified volume. For APF datasets, this may indicate a security exposure that should be investigated and corrected.
- **RACF PROTECTED**: Indicates whether the dataset has a RACF profile. The following entries may appear:
  - **YES**: Indicates that the dataset has a discrete or generic profile. If the RACF indicator for the dataset is on, the dataset is protected by a discrete profile.
  - **NO**: Indicates that no profile exists for the dataset. The dataset is not protected in any way by RACF.
- UACC is the dataset's universal access authority (UACC), if it is defined. The UACC is the default access authority that specifies how the dataset can be accessed by users or groups not in the access list of the dataset's RACF profile. Note: The UACC does not necessarily indicate the actual authority that a user has to access the dataset. The global access checking table may contain an entry applicable to the dataset, or the user may be on the access list, if the dataset has a discrete profile. The following universal access authorities may appear:
  - **ALTER**: For a dataset that is protected by a discrete profile, ALTER allows all users to read, update, or delete the dataset.
  - **CONTROL**: For VSAM (virtual storage access method) datasets, CONTROL provides all users with the same authority that is provided with the VSAM CONTROL password; that is, authority to perform control interval access (access to individual VSAM data blocks), and to retrieve, update, insert, or delete records in the specified dataset. For non-VSAM datasets, CONTROL is equivalent to UPDATE.
  - **UPDATE**: Allows all users to read or update the dataset. UPDATE does not, however, authorize a user to delete the dataset.
  - **READ**: Allows all users to access the dataset for reading or copying only.
  - **NONE**: Does not allow users to access the dataset.

Step 3

After receiving and reviewing the DSMON report to determine basic RACF controls over the datasets, you (or your data center) must then run a report to list who has access to the Medicare datasets in your environment. RACF commands should be used to provide reports of access to the Medicare datasets in your environment.

RACF Commands:

LD DA 'Medicare dataset name ' ALL GEN: This command will list the dataset definitions, showing the owner of the dataset, creation date of the dataset, group and individual IDs with access to the dataset, universal access settings (UACC) and what is audited for the dataset. This should be run for each Medicare dataset identified in Step 1 above.

LU - list user. This will list the user's default group, other groups assigned to the user, attributes assigned to the user and class authorizations. This should be run after the LD command above to list information on the users within groups that have been assigned access to Medicare datasets.

The reader will also need a listing of who the user ID has been assigned to, that is the actual name of the user, to determine which ids have been assigned to actual users and which ids are system accounts (for example, started tasks, or other IDs used to run programs, such as batch ids). Such information on the user may be part of the LU report, or may have to be obtained separately depending on the data center installation of RACF. For system accounts that have access above read to Medicare claims data files, ensure these accounts cannot be logged into by an individual user. For actual users with access above read to Medicare claims data files, verify that such access assignments are reasonable given the user's job responsibilities and document that reasoning.

Step 4[2]

After review of access assignments based on job responsibilities, if it is determined that such update access is required, logging and audit trails should be enabled to log all access to Medicare claims data files above READ. In RACF, you can use the GLOBALAUDIT operand on the ALTDSD command or request the corresponding function on the AUDIT DATASET ACCESS panel, in addition to the owner-specified logging values, to log user accesses to datasets. GLOBALAUDIT allows you to specify logging for different kinds of attempts that users make to access resources at a given access level. Through GLOBALAUDIT, you can log successful accesses, failed accesses, or both to a given resource and specify READ, UPDATE, CONTROL, or ALTER for the access level to the resource.

Note: Some authorized programs that call RACF to perform authority checking can request that RACF perform no logging. Therefore, if you request GLOBALAUDIT auditing for an access attempt made through such a program, RACF does not log the event. Similar to other specific controls, you do not audit accesses to most datasets, as a general rule. Therefore, GLOBALAUDIT(NONE) is the default for the operand. When GLOBALAUDIT(NONE) is in effect, RACF logs accesses to the dataset only as specified by the resource owner.

- **Example 1**: To use the GLOBALAUDIT operand of the ALTDSD command to direct RACF to log all accesses to dataset JIM.MEMO.TEXT, enter:

```
ALTDSD ’JIM.MEMO.TEXT’ GLOBALAUDIT(ALL(READ))
```

[2] Information from this section obtained from pages 28-29 of the z/OS Security Server RACF Auditor's Guide, V1R6.0.

- **Example 2**: To use the GLOBALAUDIT operand of the ALTDSD command to direct RACF to log all failed accesses, all successful updates, and any scratch of dataset A.B.C, enter:

  ```
  ALTDSD ’A.B.C’ GLOBALAUDIT(FAILURES(READ) SUCCESS(UPDATE))
  ```

Step 5

Establish a process and procedures for monitoring all accesses to Medicare claims data files above READ and to document the results and action taken during the review process. (Refer to RACFRPT 3-5.)

Step 6

Establish a process and procedures to periodically review access assignments allowing access above READ to Medicare claims data files to ensure such access is still required to perform job responsibilities. (Refer to RACFRPT2.)

Step 7

Establish a process to review policies and procedures used to log, monitor, and review access assignments greater than READ to Medicare claims data files at a minimum annually and update these policies and procedures as changes occur in processes.

1.1 INSTRUCTIONS FOR FI, CARRIER, OR MAC USING ACF2 MAINFRAME SECURITY

Step 1

Identify all data files containing Medicare claims data. Document file names and their contents. This may involve having the data centers review Job Control Language (JCL) to identify the data files if strong, well known naming conventions are not in place for these files. Create a process to ensure update and maintenance of file names and their contents.

Step 2[3]

Create standardized reports to document persons granted access to update Medicare claims data files. For ACF2, the ACFRPTXR Cross Reference Report should be created by your data center for the Medicare data files identified in Step 1 above. This report was created for auditors, security administrators, and management to identify which users could access which datasets and resources. You can obtain either historical information (by using backup copies of the CA-

[3] Information from this section obtained from pages 4-7, 6-4 of the CA-ACF2 Auditor's Guide, Version 6.3, page 6-18 of the CA-ACF2 Administrator Guide, Version 6.3, and pages 18-3, 18-4 of the eTrust CA-ACF2 Security for the z/OS Reports and Utilities Guide.

ACF2 datasets taken at a previous point in time) or current status (by using the online databases). Normally, this utility is used to provide a set of dataset names (such as critical system and production datasets or all datasets from the master catalog) and resource names as input to the report. The report displays a list of every system user who has any access to each dataset and resource specified. The utility identifies users that are granted access through CA-ACF2 rules, and users who are given access because of other CA-ACF2 attributes (such as security administrators, matching PREFIX field, or the NON-CNCL logonid privilege.).

An example of the ACFRPTXR report is as follows:

```
eTrust CA-ACF2 Security - ACFRPTXR - CROSS REFERENCE REPORT -PAGE 1

DATE 01/01/07 TIME 10.04 NOACF2,DSET,RRSUM,RKEY(SSS),DSN(-)

 -----------------------------------------------------------------------------------------------

DATASET: ALL RULES IN SET RKEY: SSS

STORED: 08/08/08-28:08 BY: 8888888

LOGONIDS THAT HAVE ACCESS WITHOUT RULES

ABC1234(NC)  ABC3456(NC)   ABC7890(NC)  ABC4789(NC)  ABC9075(NC)

0BRSA.- UID(*) NEXTKEY(MEDICARE)

ALL LOGONIDS MATCH SPECIFIED UID STRING

0CSAR.FIN.RNMR.PROD UID(SSS) READ(A) WRITE(L) ALLOC(L) EXEC(A)

SSSRSA     SSSR01      SSSR02      SSSR03      SSSR04      SSSR05      SSSR06
```

Acronym Definitions:

- **NOACF2**: Indicates that the report is based on alternate databases provided by the RULES, LOGONIDS, or INFOSTG input files. When alternate databases are specified as input, ACFRPTXR does not take scope records into consideration when access authorization checking is performed. ACF2 indicates that ACFRPTXR use the online eTrust CA-ACF2 clusters. The eTrust CA-ACF2 system must be active on this CPU for this type of processing.

- **DSET**: Specifies that ACFRPTXR process dataset access rules. The DSN, RKEY, and VOL input parameters might be provided using the JCL parameter field or the SYSDSLST input file.

- **RRSUM**: Specifies that the additional Rule Record Summary portion of ACFRPTXR is produced at the end of the report. This includes an entry for each rule record (that is, high-level index, $KEY value, or resource TYPE, NAME, and CLASS combination) used in producing the report. This portion of the report is also where the detailed logonid lists for each %CHANGE or %RCHANGE record encountered are displayed (assuming the LID option is also specified). Thus, when the message %CHANGE DATA EXISTS or

%RCHANGE DATA EXISTS appears in the main part of the report after the RULE KEY line, the related LID and UID entries are printed in the Rule Record Summary.

- **RKEY**: Specifies this parameter is valid only when the DSET parameter is also specified. RKEY has two uses:

  - RKEY is used with the DSN parameter to specify the key of the rule set used to validate the dataset access. This is similar to the concept of using the eTrust CA-ACF2 Dataset Prevalidation exit to perform the same function at run time. Usually, the only necessity to specify RKEY is when some rule record other than the one under the dataset high-level index is to be used for rule checking.

  - RKEY is used with a DSN parameter of dash (-) when you want to list all the rule entries for a particular key.

- **DATASET NAME(DSN)**: Specifies that ACFRPTXR uses a single dataset name without the need for the SYSDSLST file. This parameter is valid only when the DSET parameter is also specified and cannot be used with the SYSDSLST input file. The name specified must be fully qualified (regardless of time sharing option) but must not be specified in quotes. The dataset name high-level index name is used as the key to identify the applicable access rule set unless the RKEY parameter is also specified. In the case where the listing of a full rule set for a particular $KEY is desired, the DSN field must be defined as DSN(-) and the applicable $KEY value defined in the RKEY parameter.

- **Read(Allow|Log|Prevent)**: Specifies read access and the action A, L, or P that you want CA-ACF2 to take when the environment matches. Before this access permission applies, the actual access attempt must match the environment defined by other parameters of the access rule entry. The letter codes are defined as: A=Allow the access, L=Permit the access but log the event, P=Prevent the access. If not specified in the rule entry, this access permission defaults to READ(P).

- **Write(Allow|Log|Prevent)**: Specifies write access and the action (A, L, or P) that you want CA-ACF2 to take when the environment matches. This parameter works similarly to how the READ parameter does. If not specified in the rule entry, this access permission defaults to WRITE(P).

- **Allocate(Allow|Log|Prevent)**: Specifies allocate access and the action (A, L, or P) that you want CA-ACF2 to take when the environment matches. This parameter specifies that a user has create, delete, rename, and catalog authority to a dataset. If not specified in the rule entry, this access permission defaults to ALLOC(P).

- **Execute(Allow|Log|Prevent)**: Specifies execute access and the action (A, L, or P) that you want CA-ACF2 to take when the environment matches. This parameter works similarly to how the READ parameter does. However, its access permission is the specified value or the value of the READ parameter whichever designates the most permissive access. (For example, if READ(P) and EXEC(L) are specified, then EXEC(L) applies.)

If a NEXTKEY dataset is specified, you want to ensure an ACFRPTXR Cross Reference Report is also run and produced for the NEXTKEY specified. The NEXTKEY parameter directs CA-ACF2 to evaluate an alternate access rule set when a particular environment applies to the access, but the access is prevented. CA-ACF2 only checks the NEXTKEY parameter when the access matches the environment, but the rule prevents the access. Validation of the access continues with the evaluation of the alternate access rule set. To specify the index of the alternate rule set, use the NEXTKEY parameter. The NEXTKEY parameter in a rule entry lets you split a very large rule set into several sets or merge several rule sets together. You can also use NEXTKEY to delegate rule maintenance authority with the %CHANGE and %RCHANGE control statements.

Step 3

After receiving the ACFRPTXR report regarding access to the data files determined in Step 1, extract ids with access above read to Medicare claims data files. The reader will need a listing of who the user ID has been assigned to, that is the actual name of the user, to determine which ids have been assigned to actual users and which ids are system accounts(for example, started tasks, or other IDs used to run programs, such as batch ids). For system accounts that have access above read to Medicare claims data files, ensure these accounts cannot be logged into. For actual users with access above read to Medicare claims data files, verify that such access assignments are reasonable given the user's job responsibilities and document that reasoning.

Step 4[4]

After review of access assignments based on job responsibilities, if it is determined that such update access is required, logging and audit trails should be enabled to log all access to Medicare claims data files above READ. Access and resource rules control the production of the logging reports and audit trails of dataset or resource access. In all cases, you can specify a rule authorizing an access in one of two ways: ALLOW (permitting access or use and creating no report \ records), or LOG (granting the access but creating a logging report record). These permissions in rule records either create logging records (LOG) or do not (ALLOW), regardless of whether CA-ACF2 is in LOG, WARN, RULE, or ABORT mode (no records are created in QUIET mode). In other words, an access matching a rule with an ALLOW permission does not create a logging record even in LOG mode; however access matching a rule with a LOG permission will create a logging record. You can write rules at various levels of detail and specify various conditions. CA-ACF2 creates logging records for almost any set of circumstances. Rules can readily change (authorized people can modify rules dynamically using CA-ACF2 TSO commands).

The following rule set allows all users whose UIDs begin with AB to write and allocate to the dataset PROD.DATASET.NR1. Updates (write & allocate) made by these users are logged as indicated by the (L) in the parenthesis beside the permissions.

```
$KEY(PROD)

DATASET.NR1 UID(AB) WRITE(L) ALLOC(L)
```

[4] Information from this section obtained from pages 6-1, 6-5 of the CA-ACF2 Auditor's Guide, Version 6.3.

Step 5

Establish a process and procedures for monitoring all accesses to Medicare claims data files above READ and to document the results and action taken during the review process.

Step 6

Establish a process and procedures to periodically review access assignments allowing access above READ to Medicare claims data files to ensure such access is still required to perform job responsibilities.

Step 7

Establish a process to review policies and procedures used to log, monitor, and review access assignments greater than READ to Medicare claims data files at a minimum annually and update these policies and procedures as changes occur in processes.

4 THE DATA CENTER ROLE

To assist in the review of direct data access, it will be the responsibility of each data center, on a quarterly basis to develop and distribute access control reports and logs for each user from supported Fiscal Intermediaries, Carriers, DMERCs or MACs. Data centers should schedule conference calls with the supported contractors to check on the receipt of the documentation, identify and explain naming conventions, standards and preset numbers/identifiers etc. used in the reports and logs to ensure understanding on the part of contractor staff assigned to review the reports and audit logs.

5 DOCUMENTATION REQUIREMENTS

In the review of direct data access to Medicare claims data files, Fiscal Intermediaries, Carriers, Durable Medical Equipment Regional Carriers, and Medicare Administrative Contractors will be responsible for the following documentation requirements:

- Maintaining current naming conventions and standards for Medicare claims data files.
- Maintaining a current list of individuals with access above READ to Medicare claims data files with these individuals job responsibilities documented.
- Maintaining current policies and procedures for logging, monitoring, and reviewing access above READ to Medicare claims data files.
- Maintaining evidence of the periodic review of direct data access activity to include updates and violations, such as successful updates to the data itself (outside the application) and violations (attempts to access/update the data which are not allowed).

- Maintaining evidence of the periodic review of access assignments above READ.
- Providing a quarterly attestation to CMS that all access control reports and logs have been reviewed and validated.

6 CONCLUSION

Direct access to Medicare data creates a significant risk of unauthorized modifications to claims data for each and every CMS contractor. Restricting data access to only authorized users, and only in the manner intended, requires sound procedures and controls for granting and monitoring direct update access. Using the instructions identified in this white paper, Fiscal Intermediaries, Carriers, Durable Medical Equipment Regional Carriers, and Medicare Administrative Contractors will be able to build sound controls around direct update access to Medicare claims data.

Note that this whitepaper covers direct access to data and that direct access to data is not a function of the application itself. Such access presents a direct threat to the integrity and reliability of the data if sufficient controls have not been designed and implemented to ensure all changes made via direct access are proper. Because direct access to data circumvents controls built into applications (edits, audit trails, reconciliations), changes made directly to the data are inherently more risky than changes made through applications.

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

ACF2	Access Control Facility 2
APF	Authorized Program Facility
CMS	Centers for Medicare & Medicaid Services
DMERC	Durable Medical Equipment Regional Carriers
DSN	Dataset Name
FI	Fiscal Intermediaries
FISS	Financial Intermediary Standard System
FTP	File Transfer Protocol
GSO	Global System Options
HHS	Department of Health and Human Services
MAC	Medicare Administrative Contractors
MCS	Multi Carrier System
PwC	PricewaterhouseCoopers
RACF	Resource Access Control Facility
TSO	Time Share Option
VMS	VIPS Medicare System

APPENDIX C – REVIEW PROCESS DIAGRAM

Figure 1 Review Process Diagram

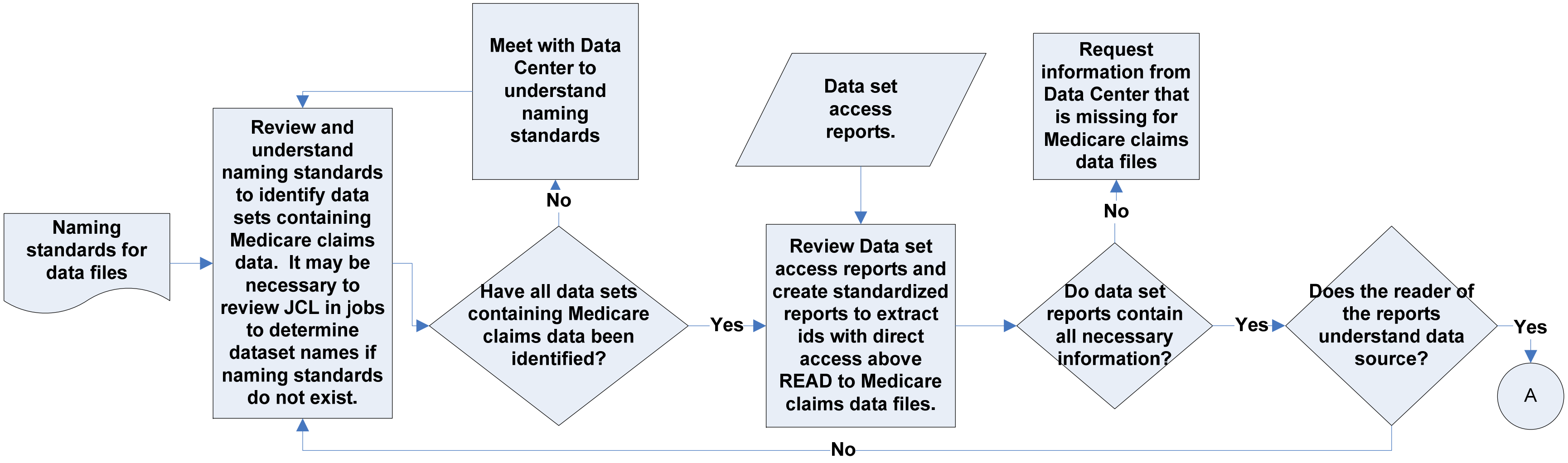
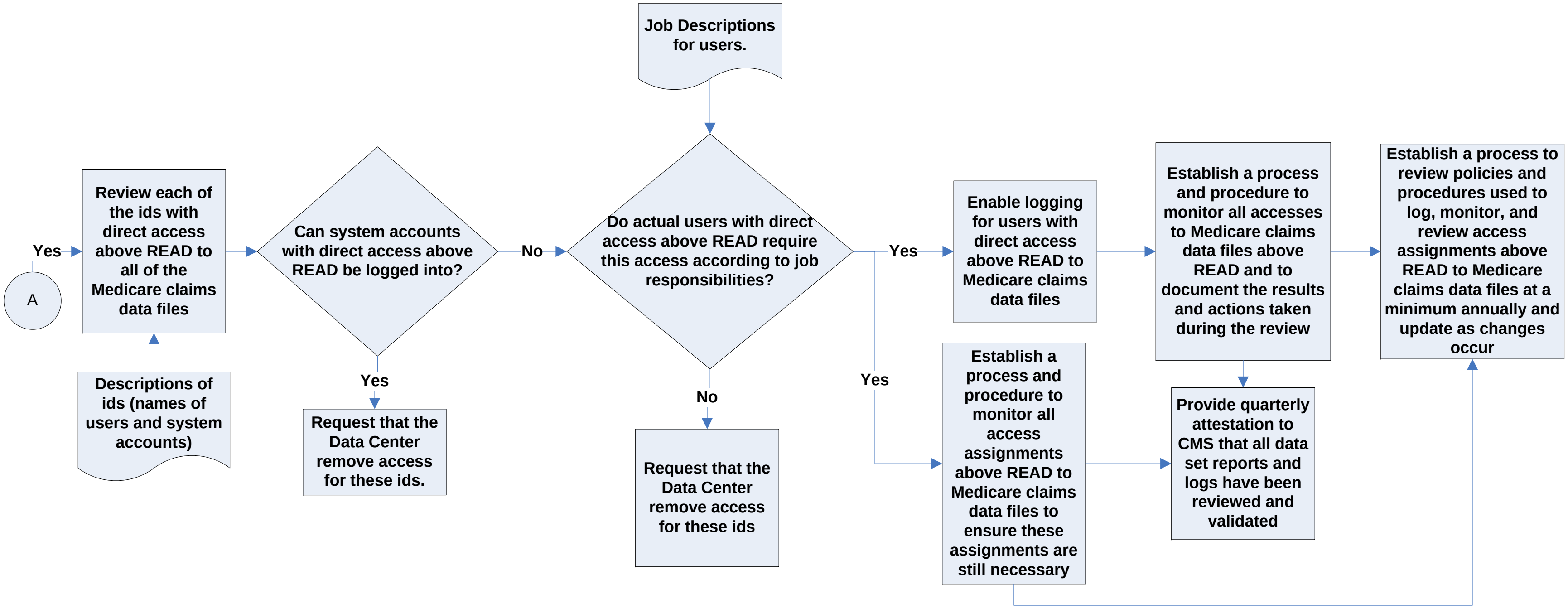
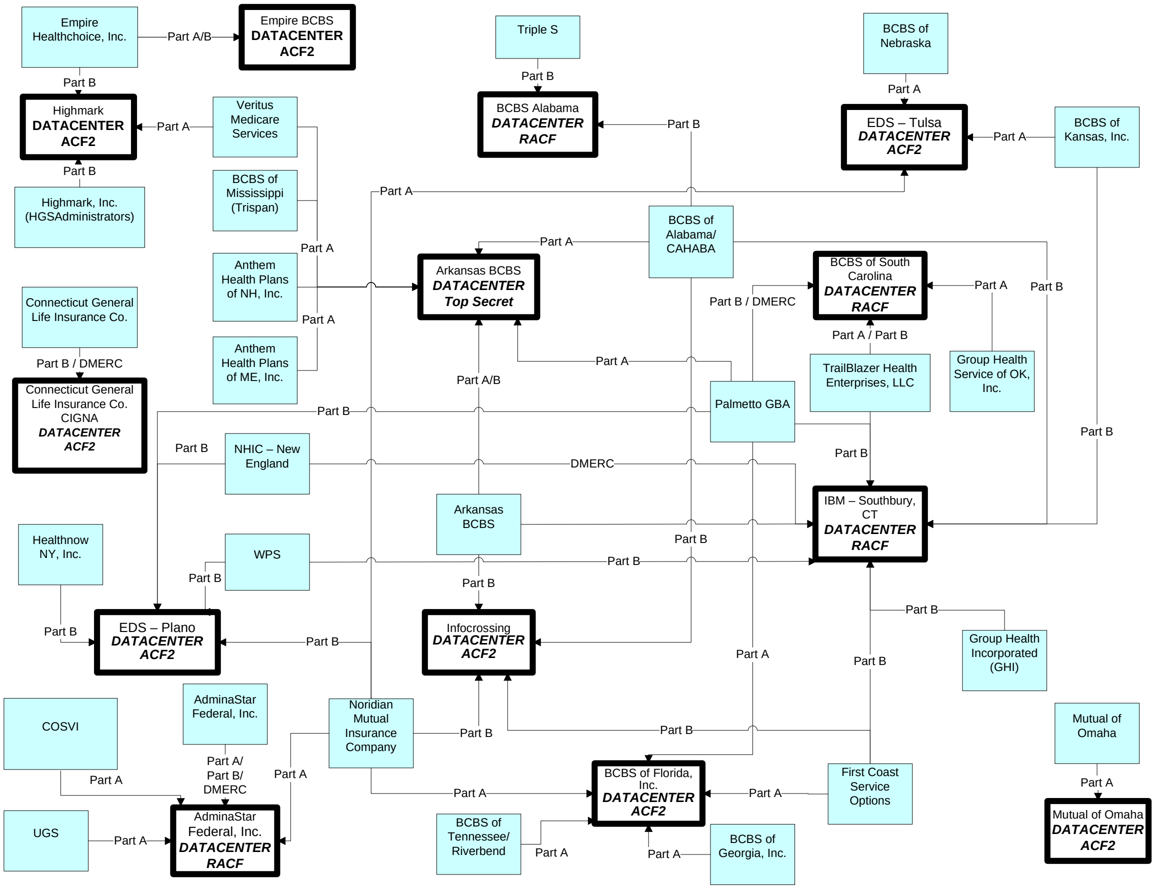

Naming standards for data files
Review and understand naming standards to identify data sets containing Medicare claims data. It may be necessary to review JCL in jobs to determine dataset names if naming standards do not exist.
Meet with Data Center to understand naming standards
No
Have all data sets containing Medicare claims data been identified?
Yes
Data set access reports.
Review Data set access reports and create standardized reports to extract ids with direct access above READ to Medicare claims data files.
Request information from Data Center that is missing for Medicare claims data files
No
Do data set reports contain all necessary information?
Yes
Does the reader of the reports understand data source?
Yes
A
No

Figure 2 Review Process Diagram


Job Descriptions for users.
A
Yes
Review each of the ids with direct access above READ to all of the Medicare claims data files
Descriptions of ids (names of users and system accounts)
Can system accounts with direct access above READ be logged into?
Yes
Request that the Data Center remove access for these ids.
No
Do actual users with direct access above READ require this access according to job responsibilities?
No
Request that the Data Center remove access for these ids
Yes
Enable logging for users with direct access above READ to Medicare claims data files
Yes
Establish a process and procedure to monitor all access assignments above READ to Medicare claims data files to ensure these assignments are still necessary
Establish a process and procedure to monitor all accesses to Medicare claims data files above READ and to document the results and actions taken during the review
Provide quarterly attestation to CMS that all data set reports and logs have been reviewed and validated
Establish a process to review policies and procedures used to log, monitor, and review access assignments above READ to Medicare claims data files at a minimum annually and update as changes occur

APPENDIX D - DATA CENTER FLOW

Figure 3 Data Center Flow


Empire Healthchoice, Inc.
Part A/B
Empire BCBS DATACENTER ACF2
Triple S
BCBS of Nebraska
Part B
Highmark DATACENTER ACF2
Part A
Veritus Medicare Services
Part B
BCBS Alabama DATACENTER RACF
Part B
Part A
EDS – Tulsa DATACENTER ACF2
Part A
BCBS of Kansas, Inc.
Part B
Highmark, Inc. (HGSAdministrators)
BCBS of Mississippi (Trispan)
Part A
BCBS of Alabama/ CAHABA
Part A
Part A
Anthem Health Plans of NH, Inc.
Arkansas BCBS DATACENTER Top Secret
BCBS of South Carolina DATACENTER RACF
Part A
Part B
Connecticut General Life Insurance Co.
Part B / DMERC
Part A
Part A / Part B
Anthem Health Plans of ME, Inc.
Part A
Part A/B
TrailBlazer Health Enterprises, LLC
Group Health Service of OK, Inc.
Part B / DMERC
Connecticut General Life Insurance Co. CIGNA DATACENTER ACF2
Part B
Palmetto GBA
Part B
Part B
NHIC – New England
DMERC
Part B
Arkansas BCBS
IBM – Southbury, CT DATACENTER RACF
Healthnow NY, Inc.
WPS
Part B
Part B
Part B
Part B
Part B
EDS – Plano DATACENTER ACF2
Part B
Infocrossing DATACENTER ACF2
Part A
Part B
Group Health Incorporated (GHI)
AdminaStar Federal, Inc.
COSVI
Noridian Mutual Insurance Company
Part B
Part B
Mutual of Omaha
Part A/ Part B/ DMERC
Part A
Part A
Part A
BCBS of Florida, Inc. DATACENTER ACF2
Part A
First Coast Service Options
Part A
UGS
Part A
AdminaStar Federal, Inc. DATACENTER RACF
BCBS of Tennessee/ Riverbend
Part A
Part A
BCBS of Georgia, Inc.
Mutual of Omaha DATACENTER ACF2

APPENDIX E - SECURITY REPORTS BY CONTRACTOR

AdminaStar Federal, Inc	
AdminaStar Federal, Inc.	RACF

Anthem Health Plans of ME, Inc.	
Arkansas Blue Cross and Blue Shield	Top Secret

Anthem Health Plans of NH, Inc.	
Arkansas Blue Cross and Blue Shield	Top Secret

Arkansas Blue Cross and Blue Shield	
Arkansas Blue Cross and Blue Shield	Top Secret
IBM	RACF
Infocrossing	ACF2

Blue Cross and Blue Shield of Alabama (CAHABA)	
Arkansas Blue Cross and Blue Shield	Top Secret
Blue Cross and Blue Shield of Alabama	RACF
IBM	RACF
Infocrossing	ACF2

Blue Cross and Blue Shield of Georgia, Inc.	
Blue Cross and Blue Shield of Florida, Inc.	ACF2

Blue Cross and Blue Shield of Kansas, Inc.	
IBM	RACF
EDS Tulsa	ACF2

Blue Cross and Blue Shield of Nebraska, Inc.	
EDS Tulsa	ACF2

CIGNA	
CIGNA	ACF2

COSVI	
AdminaStar Federal, Inc.	RACF

Empire Healthchoice, Inc.	
Empire Healthchoice, Inc.	ACF2
Highmark, Inc.	ACF2

First Coast Service Options	
Blue Cross and Blue Shield of Florida, Inc.	ACF2
IBM	RACF
Infocrossing	ACF2

Group Health Incorporated (GHI)	
IBM	RACF

Group Health Service of Oklahoma	
Blue Cross and Blue Shield of South Carolina	RACF

Healthnow NY, Inc.	
EDS Plano	ACF2

Highmark, Inc.	
Highmark, Inc.	ACF2

Mutual of Omaha	
Mutual of Omaha	ACF2

NHIC	
EDS Plano	ACF2
IBM	RACF

Noridian Mutual Insurance Company	
AdminaStar Federal, Inc.	RACF
Blue Cross and Blue Shield of Florida, Inc.	ACF2
EDS Plano	ACF2

Noridian Mutual Insurance Company	
Infocrossing	ACF2
EDS Tulsa	ACF2

Palmetto, GBA	
Arkansas Blue Cross and Blue Shield	Top Secret
Blue Cross and Blue Shield of Florida, Inc.	ACF2
Blue Cross and Blue Shield of South Carolina	RACF
EDS Plano	ACF2
IBM	RACF

Riverbend	
Blue Cross and Blue Shield of Florida, Inc.	ACF2

TrailBlazer Health Enterprises, LLC	
Blue Cross and Blue Shield of South Carolina	RACF
IBM	RACF

Triple, S	
Blue Cross and Blue Shield of Alabama	RACF

Trispan	
Arkansas Blue Cross and Blue Shield	Top Secret

UGS	
AdminaStar Federal, Inc.	RACF

Veritus Medicare Services	
Arkansas Blue Cross and Blue Shield	Top Secret
Highmark, Inc.	ACF2

Wisconsin Physician Services	
EDS Plano	ACF2
IBM	RACF

7 REFERENCES

- CA-ACF2 Administrator Guide, Version 6.3
- CA-ACF2 Auditor Guide, Version 6.3
- eTrust CA-ACF2 Security for z/OS Reports and Utilities Guide, Version 6.5
- z/OS Security Server RACF Auditor's Guide, V1R6.0
- CA - Top Secret User Guide, Release 5.1, OS/390

(This Page Intentionally Blank)