

Centers for Medicare & Medicaid Services (CMS)

Business Partners

Systems Security Manual



CENTERS FOR MEDICARE & MEDICAID SERVICES

7500 SECURITY BOULEVARD

BALTIMORE, MD 21244-1850

(Rev. 11)

CMS/ Business Partners Systems Security Manual

Record of Changes

(Rev. 11)

Revision	Major Changes	Date
<i>11</i>	<p><i>Main Document and all Appendices:</i></p> <ul style="list-style-type: none"><i>(1) CISS references removed throughout document and replaced with CFACTS.</i><i>(2) Changed email to e-mail throughout document.</i><i>(3) Changed CMS POA&M and Annual FISMA Assessment using CISS Guideline to CFACTS Guideline.</i><i>(4) Project Officer (PO) changed to Contract Officer Technical Representative (COTR) throughout document.</i> <p><i>1: Updated grammar and hyperlink to legislative resources document.</i></p> <p><i>1.1: Evaluation and test changed to security control assessment. Accreditation changed to authorization.</i></p> <p><i>2.1: Second bullet deleted.</i></p> <p><i>3: FISMA U.S. Code reference added. Contact addresses updated.</i></p> <p><i>Table 3.1: CPIC and CFACTS text added. Additional bullets added to 3.6 and 3.8 Authorization to Operate row added.</i></p> <p><i>3 Legend: CISS line item deleted. CFACTS and COTR added.</i></p> <p><i>Footnote 5: NIST reference updated.</i></p> <p><i>3.1: FISMA and Privacy Act reference added. CFACTS text added. SSP hyperlink updated. CyberTyger deleted and e-mail address changed.</i></p> <p><i>3.2: RA hyperlink updated. Grammar update. CFACTS text added. CyberTyger deleted and e-mail address changed.</i></p> <p><i>3.3: Bullet text deleted and POA&M reference updated.</i></p> <p><i>3.4: CFACTS text added.</i></p>	<i>09-30-11</i>

Revision	Major Changes	Date
	<i>3.5: Grammar update.</i>	
	<i>3.5.1: Updated wording for clarity.</i>	
	<i>3.5.2: CFACTS text added. File changed to report.</i>	
	<i>3.5.2.1: Updated wording for clarity.</i>	
	<i>3.5.2.2: Updated wording for clarity.</i>	
	<i>3.5.3: Updated wording for clarity.</i>	
	<i>3.6.1: CMS hyperlink updated.</i>	
	<i>Table 3.2: CAT 5 name updated to reflect NIST wording. NIST reference updated.</i>	
	<i>3.8: ATO section added. Subsequent sections renumbered accordingly.</i>	
	<i>3.10: CERT hyperlink added. NIST reference updated.</i>	
	<i>3.11.1: added quarterly Baseline Configuration submission info.</i>	
	<i>3.11.2: Hyperlinks updated.</i>	
	<i>3.11.3: Dates deleted. Help desk e-mail address changed.</i>	
	<i>3.11.4: Table 3.4 wording deleted. NIST hyperlink added.</i>	
	<i>Table 3.4: Deleted</i>	
	<i>4.1.1: Table 4.1 wording deleted.</i>	
	<i>Table 4.1: Deleted</i>	
	<i>4.1.2: Updated wording for clarity.</i>	
	<i>Table 4.2: Deleted</i>	
	<i>4.1.3: Table 4.2 reference deleted. CMS System Security and e-Authentication Assurance Levels by Information Type document referenced.</i>	

Revision	Major Changes	Date
-----------------	----------------------	-------------

4.1.4: NIST references updated.

Table 4.3: Renamed to Table 4.1.

4.3: Changed CMS Policy for the Information Security Program (PISP) reference and wording to reflect the most recent version. MP-5(1) control enhancement reference deleted per being moved to MP-5 in NIST 800-53 Rev. 1.

5: Changed ST&E to Security Control Assessment. Changed C&A to Security Authorization. NIST references updated. Numbering style and format update. Second bullet with hyperlink not working deleted. Internet capitalized.

Appendix A: References and links updated to reflect most current document available.

Appendix C: Deleted. References removed throughout document.

CMS/Business Partners Systems Security Manual

Table of Contents

(Rev. 11)

- 1 Introduction*
 - 1.1 Additional Requirements for MACs*
- 2 IT Systems Security Roles and Responsibilities*
 - 2.1 CMS Contract Officer Technical Representative (COTR)*
 - 2.2 Principal Systems Security Officer (SSO)*
 - 2.3 Business Owners*
 - 2.4 System Maintainers/Developers*
 - 2.5 Personnel Security/Suitability*
- 3 IT Systems Security Program Management*
 - 3.1 System Security Plan (SSP)*
 - 3.2 Risk Assessment*
 - 3.3 Certification*
 - 3.4 Information Technology (IT) Systems Contingency Plan*
 - 3.5 Compliance*
 - 3.5.1 Annual FISMA Assessment (FA)*
 - 3.5.2 Plan of Action and Milestones (POA&M)*
 - 3.5.2.1 Background*
 - 3.5.2.2 POA&M Package Components/Submission Format*
 - 3.5.3 Annual/Yearly Compliance Condition*
 - 3.6 Security Incident Reporting and Response*
 - 3.6.1 Computer Security Incident Response*
 - 3.7 System Security Profile*
 - 3.8 Authorization To Operate*
 - 3.9 Fraud Control*
 - 3.10 Patch Management*
 - 3.11 Security Management Resources*

- 3.11.1 Security Configuration Management*
- 3.11.2 Security Technical Implementation Guides (STIG)*
- 3.11.3 DHHS Federal Desktop Core Configuration (FDCC) Standard*
- 3.11.4 National Institute of Standards and Technology (NIST)*
- 4 Information and Information Systems Security*
 - 4.1 Security Objectives*
 - 4.1.1 Potential Security Impact Level*
 - 4.1.2 Security Level by Information Type*
 - 4.1.3 CMS Security Level Designation—HIGH*
 - 4.1.4 Minimum System Security Requirements—HIGH*
 - 4.2 Sensitive Information Protection Requirement*
 - 4.2.1 Restricted Area*
 - 4.2.2 Security Room*
 - 4.2.3 Secured Area (Secured Interior/Secured Perimeter)*
 - 4.2.4 Container*
 - 4.2.4.1 Locked Container*
 - 4.2.4.2 Security Container*
 - 4.2.4.3 Safe/Vault*
 - 4.2.5 Locking System*
 - 4.2.6 Intrusion Detection System (IDS)*
 - 4.2.7 Minimum Protection Alternatives*
 - 4.3 Encryption Requirements for Data Leaving Data Centers*
- 5 Internet Security*

Appendices

(Rev. 11)

Appendix A Medicare Information Technology (IT) Systems Contingency Planning

Appendix B An Approach to Fraud Control

1 Introduction

(Rev. 11)

The Centers for Medicare & Medicaid Services (CMS) requires that its business partners implement information security (IS) controls on their information technology (IT) systems to maintain the confidentiality, integrity, and availability (CIA) of Medicare systems' operations in the event of computer incidents or physical disasters.

A CMS business partner (contractor) is a corporation or organization that contracts with CMS to process or support the processing of Medicare fee-for-service claims. These business partners include Medicare carriers, Fiscal Intermediaries (FIs), Common Working File (CWF) host sites, standard system maintainers, regional laboratory carriers, claims processing data centers, Data Centers, Enterprise Data Centers (EDCs), and Medicare Administrative Contractors (MACs) (including Durable Medical Equipment Medicare Administrative Contractors [DMEMAC] and Part A/Part B Medicare Administrative Contractors [ABMAC]).

The "Medicare Prescription Drug, Improvement, and Modernization Act of 2003 (MMA)-SEC. 912: Requirements for Information Security for Medicare Administrative Contractors" (Section 912 of the MMA) provided for a new type of contractor relationship, the "Medicare Administrative Contractor," and implemented requirements for annual evaluation, testing, and reporting on security programs at both MACs and existing carrier and intermediary business partners (to include their respective data centers). In this manual the terms "business partner" and "contractor" are used interchangeably, and all provisions that apply to business partners also apply to MACs.

This manual addresses the following key business partner security elements:

- An overview of primary roles and responsibilities
- A program management planning table to assist System Security Officers (SSOs) and other security staff in coordinating system security programs at business partner sites
- The collection of CMS policies, procedures, standards, and guidelines found on the CMS IS "Virtual Handbook" Web site at: <http://www.cms.hhs.gov/InformationSecurity/>

Refer to the following CMS IS "Virtual Handbook" Web page for the key public laws and federal regulations regarding, or that impact, the implementation of federal agency IS programs: https://www.cms.gov/informationsecurity/downloads/legislative_resource.pdf.

1.1 Additional Requirements for MACs

(Rev. 11)

MACs are responsible for fulfilling all existing business partner requirements. Additional requirements are specified in Section 912 of the MMA. These additional requirements include the following:

- The contractor shall correct weaknesses, findings, gaps, or other deficiencies within 90 days of receipt of the final audit or evaluation report, unless otherwise authorized by CMS.

The contractor shall comply with the CMS Information Security (IS) Certification & Accreditation (C&A) Program Procedures, policies, standards, and guidelines for contractor facilities and systems. The CMS IS C&A Program Procedures can be found on the CMS Web site at: http://www.cms.hhs.gov/InformationSecurity/14_Standards.asp#

- The contractor shall conduct or undergo an independent *security control assessment* of its system security program in accordance with Section 912 of the MMA. The first test shall be completed before the contractor commences claims payment under the contract.
- The contractor shall support CMS validation and *authorization* of contractor systems and facilities in accordance with the CMS IS C&A Program Procedures.
- The contractor shall provide annual certification, in accordance with the CMS IS C&A Program Procedures, that they have examined the management, operational, and technical controls for its systems supporting the MAC function, and consider these controls adequate to meet CMS security standards and requirements.
- The contractor shall appoint a Chief Information Officer (CIO) to oversee its compliance with the CMS IS requirements. The contractor's principal Systems Security Officer (SSO) shall be a full-time position dedicated to assisting the CIO in fulfilling these requirements.

2 IT Systems Security Roles and Responsibilities

2.1 CMS *Contract Officer Technical Representative (COTR)*

(Rev. 11)

CMS *COTRs* (generally located in CMS Central Office [CO] business components) oversee the other business partners and also have Federal Acquisition Regulation (FAR) responsibilities at data centers. The *COTR* has the following responsibilities:

- CMS point of contact for business partner IS problems
- Provider of technical assistance necessary to respond to CMS IS policies and procedures

2.2 Principal Systems Security Officer (SSO)

(Rev. 10, Issued: 07-17-09, Effective: 08-17-09, Implementation: 08-17-09)

Business partners shall designate a principal (i.e., primary) SSO qualified to manage the Medicare IS program and ensure the implementation of necessary safeguards. The SSO shall be organizationally independent of IT operations. The SSO can be within the CIO organizational domain but cannot have responsibility for operation, maintenance, or development.

The principal SSO position for each contractor should be full-time and fully qualified—preferably credentialed in systems security (e.g., Certified Information Systems Security Professional [CISSP]). Having an individual with appropriate education and experience to execute security administration duties will help reinforce that security must be a cultural norm that guides daily activities, and not a set of compliance directives. A qualified SSO who is available to direct security operations full-time provides the foundation for the security culture and awareness of the organization.

A sound entity-wide security program is the cornerstone of effective security control implementation and maintenance. Security controls cannot be effective without a robust entity-wide security program that is fully sponsored and practiced by senior management, and staffed by individuals with proper training and knowledge. Contractors should also encourage their systems security personnel to pursue security accreditation using available funding.

A business partner may have additional SSOs at various organizational levels, but all security actions shall be coordinated through the principal SSO for Medicare records and operations. The SSO ensures compliance with the CMS IS Program and CMS Minimum Security Requirements (CMSRs) by:

- Facilitating the Medicare IT system IS program and ensuring that necessary safeguards are in place and working
- Coordinating IS system activities throughout the organization
- Ensuring that IT system IS requirements are considered during budget development and execution
- Reviewing compliance of all components with the CMSRs and reporting vulnerabilities to management
- Establishing an incident response capability, investigating system security breaches, and reporting significant problems (see section 3.6) to business partner management.
- Ensuring that technical and operational IS controls are incorporated into new IT systems by participating in all business planning groups and reviewing all new systems/installations and major changes
- Ensuring that IT systems IS requirements are included in Requests for Proposal (RFP) and subcontracts involving the handling, processing, and/or analysis of Medicare data
- Maintaining IS documentation in the System Security Profile for review by CMS and external auditors
- Cooperating in all official external evaluations of the business partner's IS program
- Facilitating the completion of the IS RA (see section 3.2)
- Ensuring that an operational IT Systems Contingency Plan is in place and tested (see section 3.4)
- Documenting and updating the monthly Plan of Action and Milestones (POA&M) (see section 3.5.2). Updates may occur whenever a POA&M projected completion date passes, and/or following the issuance of new requirements, risk assessments, internal audits, and external evaluations.
- Keeping all elements of the business partner's System Security Profile secure (see section 3.7)
- Ensuring that appropriate safety and control measures are arranged with local fire, police, and health agencies for handling emergencies (see Appendix A)

The principal SSO should earn a minimum of 40 hours in continuing professional education credits each year from a recognized national information systems security organization. The educational sessions conducted at the CMS Security Best Practices Conference can be used toward fulfilling the continuing professional education credits. The qualifying sessions and associated credit hours will be noted on the CMS Security Best Practices Conference agenda.

2.3 Business Owners

(Rev. 10, Issued: 07-17-09, Effective: 08-17-09, Implementation: 08-17-09)

Business Owners of business partner systems are responsible for:

- Determining and documenting the information and information system security levels of the resources for which they are responsible
- Identifying appropriate security level categorizations for their information and information systems

2.4 System Maintainers/Developers

(Rev. 10, Issued: 07-17-09, Effective: 08-17-09, Implementation: 08-17-09)

Business partner system maintainers/developers have the responsibility to implement the security requirements throughout the System Development Life Cycle (SDLC).

2.5 Personnel Security/Suitability

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

All business partner and contractor employees requiring access to CMS sensitive information shall meet minimum personnel suitability standards. These suitability standards are based on a valid need-to-know, which cannot be assumed from position or title, and favorable results from a background check. The background check for prospective and existing employees (if not previously completed) should include, at a minimum: contacting references provided by the employee and contacting the local law enforcement agency or agencies.

3 IT Systems Security Program Management

(Rev. 11)

Business partners shall have policies and procedures, and implement controls or plans that fulfill the CMSRs (see CMS Information Security Acceptable Risk Safeguards (ARS) Including CMS Minimum Security Requirements

http://www.cms.hhs.gov/InformationSecurity/14_Standards.asp#). The business partner Medicare claims related security program shall be based on the collection of CMS policies, procedures, standards and guidelines found on the CMS IS “Virtual Handbook” Web site at: <http://www.cms.hhs.gov/InformationSecurity>.

Policies are formal, up-to-date, documented rules stated as "shall" or "will" statements that exist and are readily available to employees. They establish a continuing cycle of assessing risk and implementation and use monitoring for program effectiveness. Policies are written to cover all major facilities and operations corporate-wide or for a specific asset (e.g., Medicare claims processing), and they are approved by key affected parties. Policies delineate the IT security management structure, clearly assign IT security responsibilities, and lay the foundation necessary to reliably measure progress and compliance. Policies also identify specific penalties and disciplinary actions to be used in the event that the policy is not followed.

Procedures are formal, up-to-date, documented instructions that are provided to implement the security controls identified by the defined policies. They clarify where the action is to be performed, how the action is to be performed, when the action is to be performed, who is to perform the action, and on what the action is to be performed. Procedures clearly define IT security responsibilities and expected behaviors for: asset owners and users, information resources management and data processing personnel, management, and IT security administrators. Procedures also indicate appropriate individuals to be contacted for further information, guidance, and compliance. Finally, procedures document the implementation of, and the rigor with which, the control is applied.

Controls are measures implemented to protect the CIA of sensitive information. IS procedures and controls shall be implemented in a consistent manner everywhere that the procedure applies. Ad hoc approaches that tend to be applied on an individual or case-by-case basis are discouraged. In addition, initial testing shall be performed to ensure that IS controls are operating as intended.

Meeting requirements does not validate the quality of a program. Managers with oversight responsibility shall understand the processes and methodology behind the requirements. Table 3.1 identifies key requirements and their high-level descriptions. As appropriate, Table 3.1 refers to other parts of this document that provide details on ways to accomplish each requirement. Business partners shall perform a *Federal Information Security Management Act of 2002, 44*

*U.S.C. §3541 (FISMA) Assessment*¹ (FA) using the *CMS FISMA Controls Tracking System (CFACTS)*. The weaknesses, action plans, and POA&Ms shall be recorded in the *CFACTS* (See *CFACTS Guideline*). To perform the FA, business partners shall conduct a systematic review of the CMSRs using the *CFACTS*. *CFACTS* provides a “Control Response” form that includes guidance and assessment procedures to assist in the review of the CMSRs.

The CMSRs include key security-related tasks. Table 3.1 indicates how often these tasks need to be performed, the disposition of output or documentation, comments, and a space to indicate completion or a “do by” date. The number accompanying each entry in the requirement column indicates the section in this document that deals with that particular requirement. Use this table as a checklist to ensure that all required IT systems security tasks are completed on schedule. Consult the referenced sections for clarifying details.

Table 3.1. Reporting Requirements Planning Table

Requirement	Frequency	Send To	Comments	Complete (check when complete)
CMS POA&M & Annual FISMA Assessment	One third of the controls shall be tested each federal FY so all controls are tested during a 3-year period.	<ul style="list-style-type: none"> <i>COTR</i> with a copy to CMS CO <i>via CFACTS</i> System Security Profile 	<p>See <i>CFACTS Guideline</i> for an overview of the FA.</p> <p>FA results recorded <i>in the CFACTS</i> are to be discussed in the <i>CPIC</i> Certification Package.</p>	
3.1 Information Security (IS) System Security Plans (SSP)	The IS SSP for each GSS and MA shall be reviewed, updated, and certified by management each federal FY (minimally), or upon significant change ² .	<ul style="list-style-type: none"> SSO CMS CO <i>via CFACTS</i> System Security Profile 	IS SSPs are to be reviewed, updated, and certified by management and indicated as such in both <i>the CFACTS</i> , the <i>CPIC</i> Certification Package/Statement of Certification, and the System Security Profile ³ .	
3.2 Information Security Risk Assessment (IS RA)	The IS RA for each GSS and MA shall be reviewed, updated, and certified by management each federal FY (minimally), or upon significant change. ¹	<ul style="list-style-type: none"> CMS CO <i>via CFACTS</i> System Security Profile 	IS RAs are to be reviewed, updated, and certified by management and indicated as such in <i>the CFACTS</i> , the <i>CPIC</i> Certification Package/Statement of Certification, and the System Security Profile. The IS RA is submitted with the IS SSP ⁴ .	

¹ The former CISS FISMA Evaluation (FE) and Self-Assessment (CAST) have been replaced with the OMB mandated annual FISMA security control assessment (FISMA Assessment [FA]).

² NIST defines “significant change” as “any change that the responsible agency official believes is likely to affect the confidentiality, integrity, or availability of the system, and thus, adversely impact agency operations (including mission, functions, image or reputation) or agency assets.”

³ More information about system security planning can be found in the CMS Information Security (IS) System Security Plan (SSP) Procedures.

⁴ More information about Risk Assessment Reports can be found in the CMS Information Security Risk Assessment (IS RA) Procedures.

Requirement	Frequency	Send To	Comments	Complete (check when complete)
3.3 Certification	Each federal FY	<ul style="list-style-type: none"> <i>COTR</i> with a copy to CMS CO <i>via CFACTS</i> System Security Profile 	Fls and carriers should include a statement of certification as part of their CPIC package. Each year CMS will publish in Chapter 7 (Internal Controls) of its Financial Management Manual (Pub 100-6) information on certification requirements including where, when, and to whom these certifications shall be submitted. All other contractors should submit a statement of security certification to their CMS <i>COTRs</i> .	
3.4 IT Systems Contingency Plan (CP)	CPs shall be reviewed, updated, and certified by management each federal FY (minimally), or upon significant change. ¹ CPs shall be tested annually.	<ul style="list-style-type: none"> SSO CMS CO <i>via CFACTS</i> System Security Profile 	Management and the SSO shall approve the CP. The IT Systems CP is to be developed (in accordance with Appendix A <i>and CMS CP procedures</i>), reviewed, updated, and certified by management—and indicated as such in <i>the CFACTS, the Certification Package/Statement of Certification, and the System Security Profile</i> ⁵ .	
3.5 Compliance	Each federal FY	<ul style="list-style-type: none"> SSO <i>COTR</i> CMS CO <i>via CFACTS</i> System Security Profile 	POA&M: POA&Ms address findings of internal/external audits/reviews including <i>annual security assessments</i> , and, as applicable: SAS 70 audits, CFO controls audits, the Section 912 evaluation, and data center tests and reviews.	
3.6 Incident Reporting and Response	As necessary	<ul style="list-style-type: none"> <i>COTR</i> <i>CMS IT Service desk</i> <i>MCMG Security Mailbox (See JSM/TDL.09323)</i> System Security Profile 	HIPAA also addresses Incident Reporting information.	
3.7 System Security Profile	As necessary	On file with the Principal SSO		
3.8 Authorization To Operate	<i>As necessary to acquire and maintain a CMS CIO-granted Authorization to Operate.</i>	<i>On file with CMS Office of the Chief Information Security Officer, with a copy maintained in the CFACTS.</i>		

⁵ More information about contingency planning can be found in NIST SP 800-12, An Introduction to Computer Security: The NIST Handbook, and NIST SP 800-34 *Rev. 1*, Contingency Planning Guide for *Federal* Information Systems.

LEGEND:

<i>CFACTS</i>	<i>CMS FISMA Controls Tracking System</i>
CFO	Chief Financial Officer
CO	Central Office (CMS)
<i>COTR</i>	<i>Contract Officer Technical Representative (COTR)</i>
CP	Contingency Plan
CPIC	Certification Package for Internal Controls
FA	FISMA Assessment
FY	Fiscal Year
GSS	General Support System
HIPAA	Health Insurance Portability and Accountability Act
IS	Information Security
IT	Information Technology
MA	Major Application
POA&M	Plan of Action and Milestones
RA	Risk Assessment
SAS	Statement on Auditing Standard
SP	Special Publication (NIST)
SSO	Business Partner Systems Security Officer
SSP	System Security Plan

Note: The documents listed in *Table 3.1* may be stored as paper documents, electronic documents, or any combination thereof.

When submitting documentation to the CMS CO, Registered Mail™ or its equivalent (signed receipt required) shall be used. For supporting documentation (such as RAs, CPs, SSPs, etc.), only electronic copies in the approved CMS format are required. Paper copies are only required for certification signature pages, certifying the completion of required periodic document development, review, updates, and certification. Contact addresses are as follows:

Program Safeguard Contractors (PSC) *and Zone Program Integrity Contractors (ZPIC)*

- CMS Central Office
Center for Program Integrity
Division of Benefit Integrity Management Operations
Mail Stop C3-02-16
7500 Security Blvd.
Baltimore, MD 21244-1850

Common Working File (CWF) and Shared System Maintainers

- CMS Central Office
Office of Information Services
Business Application and Management Group
Mail Stop N3-13-27
7500 Security Blvd.
Baltimore, MD 21244-1850

Fiscal Intermediaries /Carriers/ Medicare Administrative Contractors (MACs) (including Durable Medical Equipment Medicare Administrative Contractors [DMEMAC] and A/B Medicare Administrative Contractors [ABMAC])

- CMS Central Office

Center for Medicare
Medicare Contractor Management Group
Mail Stop S1-14-17
7500 Security Blvd.
Baltimore, MD 21244-1850

Data Centers and Enterprise Data Centers (EDC)

- CMS Central Office
Office of Information Services
Enterprise Data Center Group
Mail Stop N1-19-18
7500 Security Blvd.
Baltimore, MD 21244-1850

3.1 System Security Plan (SSP)

(Rev. 11)

The objective of an IS program is to improve the protection of sensitive/critical IT resources. All business partner systems used to process, transmit, or store Medicare-related data have some level of sensitivity and require protection. The protection of a system shall be documented in an IS SSP. The completion of an SSP is a requirement of *the Federal Information Security Management Act of 2002 (FISMA), Privacy Act of 1974, As Amended*, OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, and Public Law 100-235, the Computer Security Act of 1987. All Medicare claims-related applications and systems categorized as either an MA or GSS shall be covered by SSPs.

The purpose of an SSP is to provide an overview of the security requirements of a system and describe the controls that are implemented to meet those requirements. The SSP also delineates responsibilities and expected behavior of all individuals who access the system. The SSP should be viewed as documentation of the structured process of planning adequate and cost-effective security protection for a system. It should reflect input from various managers with responsibilities concerning the system, including Business Owners, information owners, the system operator, and the system security manager (i.e., SSO).

All business partners are required to maintain current SSPs for their Medicare claims-related GSSs and MAs in *both the CFACTS and* their System Security Profiles. The SSP documents the current level of security within the system or application; that is, actual implemented controls, not planned controls. In addition, the SSP serves as the primary documentation reference for testing and evaluation, whether by CMS, the General Accounting Office (GAO), or other oversight bodies. The SSP is a sensitive document, as it may discuss uncorrected vulnerabilities

and may mention risks that have been accepted. Therefore, SSPs should be distributed only on a need-to-know basis.

The SSPs shall be available to the SSO and business partner certifying official (normally the Vice President [VP] for Medicare Operations), and authorized external auditors as required. The SSO and Business Owner are responsible for reviewing the SSP on an annual basis to ensure that it is up-to-date. The objective of these annual reviews is to verify that the controls selected or installed remain adequate to provide a level of protection to reach an acceptable level of risk to operate the system.

All business partner Medicare claims-related SSPs shall be developed in accordance with the most current version of the CMS System Security Plan (SSP) procedures available on the CMS Web site at: <http://www.cms.hhs.gov/InformationSecurity>.

SSPs shall be re-certified within 365 days from the previous certification date. The SSP shall also be reviewed prior to re-certification (within the original certification timeframe) to determine whether an update is required. The SSP shall be updated if there has been a significant change or the security posture has changed. Examples of significant change include, but are not limited to: transition from one standard system to another, replacement of major computer equipment, change in operating system used, change in system boundaries, or any significant system modifications that may impact the system's security posture. Documentation of the review or the updated SSP, if applicable, shall be *recorded in the CFACTS*, placed in the System Security Profile, and a copy shall be submitted to the CMS CO.

Contractors updating their current SSP(s) or developing new SSP(s) shall include Medicare claims processing front-end, back-end, and/or other claims processing related systems using the most current version of the CMS SSP procedures.

Front-end systems are those systems Medicare contractors develop and maintain for use in their operations areas and data centers to enter claims and claims-related data into the standard/shared claims processing system. These front-end systems include, but are not limited to: electronic data interchange, imaging systems, optical character recognition, manual claims entry, claims control, provider, beneficiary, other payer databases, and other pre-claims processing business functions.

Back-end systems are those systems that Medicare contractors develop and maintain for use in their operations areas and data centers to output claims processing information (i.e., checks, Medicare summary notices, letters, etc). These back-end systems include, but are not limited to: print mail, 1099 forms, post-payment medical reviews, customer service, appeals, overpayment written/phone inquiries and separate claims reconciliation systems.

A newly developed or updated SSP shall be *maintained in the CFACTS and* sent in electronic form to the CMS CO on CD-ROM. This CD-ROM must be received by CMS 10 working days after the SSP(s) has been developed, updated, or re-certified. The original signed, dated CMS SSP certification form shall be submitted in paper copy form along with the CD-ROM electronic

copy. This information shall not be submitted to the CMS CO via *e-mail*—Registered Mail™ or its equivalent (signed receipt required) shall be used.

In summary, the SSP shall be updated and re-certified annually unless there are changes (as discussed above) that would necessitate a more frequent update. Should SSP technical assistance be required, direct all questions to *the CMS Office of the Chief Information Security Officer* at *CISO@cms.hhs.gov*.

3.2 Risk Assessment

(Rev. 11)

Business partners are required to perform an annual risk assessment in accordance with the most current versions of the CMS Information Security Risk Assessment procedures available on the CMS Web site at: <http://www.cms.hhs.gov/InformationSecurity>.

The CMS IS RA procedures present a systematic approach for the RA process of Medicare information computer systems within the CMS and business partner environments. The procedure describes the steps required to produce an IS RA for systems and applications.

All business and information owners shall develop, implement, and maintain risk management programs to ensure that appropriate safeguards are taken to protect all CMS resources. A risk-based approach shall be used to determine adequate security and shall include a consideration of the major factors in management, such as the value of the system or application, all threats, all vulnerabilities, and the effectiveness of current or proposed safeguards. The CMS IS RA procedures shall be used to prepare an annual IS RA.

IS RAs shall be re-certified within 365 days from the previous certification date. The RA shall also be reviewed prior to re-certification (within the original certification timeframe) to determine whether an update is required. The RA shall be updated if there has been a significant change or the security posture has changed. Examples of significant change include, but are not limited to: transition from one standard system to another, replacement of major computer equipment, change in operating system used, change in system boundaries, or any significant system modifications that may impact the system's security posture. Documentation of the review or the updated RA, if applicable, shall be placed in the System Security Profile, and a copy shall be submitted to the CMS CO. Note that the RA used to support a SSP cannot be dated more than 12 months earlier than the SSP certification date.

Contractors that must update their current RA(s) shall use the most current versions of the CMS IS RA procedures.

A newly developed or updated RA that is submitted with the SSP shall be *maintained in the CFACTS and* sent to the CMS CO on CD-ROM. The CD-ROM must be received by CMS 10 working days after they have been developed and/or updated. This information shall not be submitted to the CMS CO via *e-mail*—Registered Mail™ or its equivalent (signed receipt required) shall be used.

In summary, the RA shall be updated annually unless there are changes (as discussed above) that would necessitate a more frequent update. Should RA technical assistance be required, direct all questions to *the CMS Office of the Chief Information Security Officer at CISO@cms.hhs.gov*.

3.3 Certification

(Rev. 11)

All business partners are required to certify their system security compliance. Certification is the formal process by which a contractor official verifies, initially and then by annual reassessments, that a system's security features meet the CMSRs. Business partners shall self-certify that their organization successfully completed an annual, independent FA of their Medicare IT systems and associated software in accordance with the terms of their Medicare agreement/contract.

Each contractor is required to self-certify to CMS its IS compliance within each federal FY. This security certification shall be included in the Certification Package for Internal Controls (CPIC) or, for contracts not required to submit CPICs, send the security certification to their appropriate CMS *COTRs*. CMS shall continue to require annual, formal re-certifications within each FY no later than September 30, including validation at all levels of security as described in this manual.

Systems security certification shall be fully documented and maintained in the System Security Profile. The security certification validates that the following items have been developed (i.e., updated and/or reviewed, as required) and are available for review in the System Security Profile:

- Certification
- FISMA Annual Security Control Assessment
- System Security Plan for each GSS and MA (see section 3.1)
- Risk Assessment (see section 3.2)
- IT Systems Contingency Plan (see section 3.4 and Appendix A)
- Plan of Action and Milestones (see section 3.5.2)

3.4 Information Technology (IT) Systems Contingency Plan

(Rev. 11)

All business partners are required to develop and document an IT Systems Contingency Plan (CP) that describes the arrangements that have been implemented and the steps that shall be taken to continue IT and system operations in the event of a natural or human-caused disaster. IT Systems CPs shall be included in management planning and shall be:

- Reviewed whenever new systems are planned or new safeguards contemplated
- Reviewed annually to ensure that they remain feasible
- Tested annually. If backup facility testing is done by Medicare contract type (i.e., when multiple contract types are involved [e.g., Data Center, Part A/B, DMERC]), each individual Medicare contract type shall be tested every year.

Appendix A to this manual provides information on Medicare IT systems contingency planning and testing methods. See *item* 3.4 in Table 3.1, section 3.0, for other references.

Each contractor shall review its IT Systems CP 365 days from the date it was last reviewed and/or updated to determine if changes to the CP are needed. A CP shall be updated if a significant change has occurred. The CP shall also be tested 365 days from the last test performed. Updated plans and test reports (results) shall be *maintained in CFACTS, and* placed in the contractor's System Security Profile. Business partner management and the SSO shall approve newly developed and/or updated IT Systems CP. Information on Medicare IT systems contingency planning can be found in Appendix A.

A newly developed and/or updated IT Systems CP shall be *updated in CFACTS and* submitted to CMS within 10 working days after the business partner's management and SSO have approved it. A copy of the IT Systems CP shall be submitted via CD-ROM to the CMS CO along with a paper copy of the statement of certification. This information shall not be submitted via *e-mail*—Registered Mail™ or its equivalent (signed receipt required) shall be used.

3.5 Compliance

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

Compliance refers to the contractual obligations of business partners to CMS. The components to electronic data processing (EDP) security reporting compliance are described in detail in the following subsections

3.5.1 Annual FISMA Assessment (FA)

(Rev. 11)

A critical factor for maintaining on-going compliance with FISMA and the Federal Managers' Financial Integrity Act of 1982 (FMFIA) is for Business Owners in coordination with developers/maintainers, to annually test their internal controls and dedicate sufficient resources to accomplish this test. These resources include budget (if external resources are to be used to support the testing) and person-hours (if internal personnel are to be engaged in this activity). They are required to schedule and perform the test; and oversee the development and completion of applicable POA&Ms for vulnerabilities noted during the annual testing.

The annual FA is documented, tracked, and reported in the *CFACTS*. The purpose of annual FA testing (i.e., validation) is to examine and analyze implemented security safeguards in order to provide evidence of compliance with applicable laws, directives, policies, and requirements regarding information security. The annual FA is intended to validate the CMSRs to determine the extent to which the controls are:

- implemented correctly
- operating as intended
- producing the desired outcome with respect to meeting the security requirements for the system

The annual FA testing requirement has been interpreted by OMB as being within 365 calendar days of the prior test. Over a 3-year period, all CMSRs applicable to a system or application shall be tested. This means a subset (no less than one-third [$\frac{1}{3}$]) of the CMSRs shall be tested each year so that all security controls are tested during a 3-year period.

CMS CO reserves the right to mandate which subset of CMSRs must be tested during any given year. CMS *also* requires that all CMSRs be tested within a 3-year period. Business Owners, in coordination with the developers/maintainers of CMS applications and systems, are responsible for meeting this requirement.

To fulfill the annual FA validation obligation, the FA shall be conducted by an independent agent or team. This can be any internal/external agent or team that is capable of conducting an impartial assessment of an organizational information system. Impartiality implies that the assessors are free from any perceived or actual conflicts of interest with respect to the development, operation, and/or management chain of command associated with the information

system or to the determination of CMSR effectiveness. All management-directed and independent testing conducted with 365 days of the attestation due date may be used to meet the requirement for the annual security controls (i.e., FA) testing.

3.5.2 Plan of Action and Milestones (POA&M)

(Rev. 11)

Business partners are required to prepare a monthly POA&M update which is due by the 1st of each month. The POA&M update consists of updating all active POA&M items in the *CFACTS* and, if required by CMS, uploading any additional supporting documentation.

3.5.2.1 Background

(Rev. 11)

FISMA requires that federal agencies provide annual reporting of the state of security programs for all IT systems associated with the agency. Additionally, periodic POA&Ms reporting the status of known security weaknesses for all federal agency systems shall also be submitted to the OMB. This reporting requirement applies to a broader scope of security weaknesses, as it is not limited to weaknesses identified by specific audits and reviews (such as those covered under FMFIA). In the case of FISMA, any security weakness identified for any covered system shall be reported and included in a periodic POA&M report.

Section 912 of the MMA implemented requirements for annual evaluation, testing, and reporting on security programs for both MACs and existing carrier and FI business partners (to include their respective data centers). These Section 912 evaluations and reports necessitate an annual on-site review of business partner security programs to ensure that they meet the information security requirements imposed by FISMA. CMS, as part of its overall FISMA reporting obligations, requires that corrective actions for identified deficiencies (i.e., weaknesses) be addressed in a report to be submitted shortly after the evaluation results are finalized, as well as periodically thereafter to track updated progress towards completion of the identified action plans.

The *CFACTS* enables contractors to satisfy reporting requirements for EDP security-related findings. Security-related findings and approved action plan data is *promptly* entered into the *CFACTS* following all audits/reviews, from which the *CFACTS provides* a single monthly submission *report* that summarizes the current state of security for the business partner.

3.5.2.2 POA&M Package Components/Submission Format

(Rev. 11)

In addition to the initial POA&M reporting that follows each audit/review, summary POA&Ms *will be generated* on the 1st of each month, *based on the data maintained in the CFACTS*. The *CFACTS* shall be populated *and maintained* with security-related findings *and action plans* from any audit or review, whether internal or external. Corrective actions are to be established in the *CFACTS* to address all resulting weaknesses entered therein, and those corrective actions shall be *maintained current* in the *CFACTS to support the monthly reporting requirements*.

Initial Report. Within 30 days (or as otherwise directed by CMS) of the final results for every internal/external audit/review, an initial CMS POA&M is due to CMS that describes the findings of the audit/review and initial corrective actions planned for implementation.

Monthly POA&M Package. On a monthly basis, business partners shall provide updates *in the CFACTS* on progress towards completion of remediation efforts for weaknesses identified from all known sources.

3.5.3 Annual/Yearly Compliance Condition

(Rev. 11)

Many security documents, such as IS RAs, SSPs, Contingency Plans, as well as many CMSR control *requirements* (see CMS Information Security Acceptable Risk Safeguards [ARS], CMS Minimum Security Requirements Appendices A, B, and C) require annual or yearly performance (e.g., test, submission, recertification, review, update). When such a requirement is to be performed annually or yearly, it is to be performed no later than the one year anniversary date of its previous performance (i.e., within 365 days [366 days in leap years]). The only exceptions to this annual/yearly compliance condition are deliverables whose annual due date are set and distributed by CMS, such as the annual FA submission.

If the business partner wishes to change the timing cycle of an annual or yearly requirement compliance date, the business partner *is required to* shorten the timing cycle and not lengthen the annual/yearly timing cycle to attain the new performance date. For example, if the annual/yearly performance date for reviewing the SSP is 7/31/06 and the business partner desired to change the review date to 5/31/07, they would be required to review the SSP no later than 7/31/06 and again no later than 5/31/07, and no later than 5/31/yy thereafter.

3.6 Security Incident Reporting and Response

(Rev. 10, Issued: 07-17-09, Effective: 08-17-09, Implementation: 08-17-09)

A security incident is the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. It also means the loss of data through theft or device misplacement, loss or misplacement of hardcopy documents and misrouting of mail, all of which may have the potential to put the data at risk of unauthorized access, use, disclosure, modification, or destruction.

The business partner shall use its security policy and procedures to determine whether the security incident is reportable (as defined in Table 3-3). Upon receiving notification of an IT systems security incident or a suspected incident, the SSO shall immediately perform an analysis to determine if an incident actually occurred. The incident could result in adversely impacting the processing of Medicare data or the privacy of Medicare data. Reportable incidents include:

- **Unauthorized Disclosure:** Information disclosure with risk to privacy information or public relations impact
- **Denial of Service:** An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources
- **Malicious Code:** A virus, worm, Trojan horse, or other code-based malicious entity that infects a host
- **Unauthorized Access:** A breach in which person gains logical or physical access to network, system application, data or other resource without permission
- **Inappropriate Usage:** A violation of acceptable computing use policies
- **Multiple Components:** A single incident that encompasses two or more incidents

3.6.1 Computer Security Incident Response

(Rev. 11)

All suspected information security incidents or events shall be reported to the business partner IT service desk (or equivalent business partner function) as soon as an incident comes to the attention of an information system user. All confirmed security incidents and events shall be reported to the CMS IT Service Desk in accordance with the procedures set forth in the CMS Information Security Incident Handling and Breach Analysis/Notification Procedure. This

document is available on the CMS Web site at <http://www.cms.hhs.gov/InformationSecurity>. The CMS IT Service Desk can be contacted by telephone at 410-786-2580 or by e-mail at: CMS_IT_Service_Desk@cms.hhs.gov.

All CMS contractors and business partners shall utilize the following incident categories, Table 3.2, and reporting time criteria, Table 3.3, when reporting incidents to CMS.

Table 3.2. Incident Categories

Category	Name	Description
CAT 0	Exercise /Network Defense Testing	Used during state, federal, national, international exercises, and approved activity testing of internal/external network defenses or responses.
CAT 1	Unauthorized Access*	A person gains logical or physical access without permission to a network, system, application, data, or other resource.
CAT 2	Denial of Service*	An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources.
CAT 3	Malicious Code*	A virus, worm, Trojan horse, or other code-based malicious entity that infects a host.
CAT 4	Inappropriate Usage*	A person violates acceptable computing use policies.
CAT 5	<i>Scans/Probes/ Attempted Access</i>	This category includes any activity that seeks to access or identify a federal agency computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service.
CAT 6	Investigation	Unconfirmed incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.

Category	Name	Description
PII	Personally Identifiable Information (PII) Exposure	<p>Any information about an individual including, but not limited to, education, financial transactions, medical history, and criminal or employment history, and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information, which is linked or linkable to an individual.</p> <p>Any incident that involves compromised PII must be reported within 1 hour of detection regardless of the incident category reporting timeframe.</p>

*Source: NIST SP 800-61 *Rev. 1*

Table 3.3. Incident Reporting Timeframe Criteria

Category	Reporting Timeframe
CAT 0	Not applicable; this category is for CMS' internal use during exercises.
CAT 1	Within one hour of discovery/detection.
CAT 2	Within two hours of discovery/detection if the successful attack is still ongoing and the agency is unable to successfully mitigate activity.
CAT 3	Daily; within one hour of discovery/detection if widespread across agency.
CAT 4	Weekly.
CAT 5	Not applicable; this category is for classified systems.
CAT 6	Not applicable; this category is for CMS' use to categorize a potential incident that is currently being investigated.
PII	Within one hour of discovery/detection.

When reporting confirmed security incidents, business partners shall report the date and time when events occurred or were first discovered; names of systems, programs, or networks effected by the incident; and impact analysis. Release of information during incident handling shall be on an as-needed and need-to-know basis. When other entities should be notified of incidents at external business partner sites, CMS will coordinate with legal and public affairs contacts at the effected entities. If a violation of the law is suspected, CMS will notify the OIG Computer Crime Unit and submit a report to the Federal Computer Incident Response Capability (FedCIRC) of the incident with a copy to the CMS Senior Information Systems Security Office.

As part of the risk management process, the business partner shall determine the extent of the incident's impact and the potential for new or enhanced controls required to mitigate newly

identified threats. These new security controls (and associated threats and impacts) should provide additional input into the business partner's risk assessment. Business partners shall refer to The CMS Information Security Incident Handling and Breach Analysis/Notification Procedure for further guidance.

3.7 System Security Profile

(Rev. 10, Issued: 07-17-09, Effective: 08-17-09, Implementation: 08-17-09)

Consolidate security documentation (paper documents, electronic documents, or a combination) into a System Security Profile that includes the following items:

- Completed FAs
- IS System Security Plans (for each GSS and MA)
- IS Risk Assessments
- Certifications
- IT Systems Contingency Plans
- POA&Ms for each compliance security review
- POA&Ms for other security review undertaken by DHHS OIG, CMS, Internal Revenue Service (IRS), GAO, consultants, subcontractors, and business partner security staff
- Incident reporting and responses
- Systems IS policies and procedures

The System Security Profile shall be kept in a secure location, kept up-to-date, and pointers to other relevant documents maintained. A backup copy of the System Security Profile shall be kept at a secure off-site storage location, preferably at the site where back-up tapes and/or back-up facilities are located. The back-up copy of the profile shall also be kept up-to-date, particularly the contingency plan documents.

3.8 Authorization To Operate

(Rev. 11)

Business partners are required to acquire and maintain a CMS CIO-issued Authorization to Operate (ATO) for each GSS and MA. The guide for Authorization To Operate is defined in the CMS IS Authorization To Operate Package Guide document, located at:

https://www.cms.gov/informationsecurity/downloads/ATO_Package_Guide.PDF

3.9 Fraud Control

(Rev. 11)

Business partners are required to safeguard systems against fraud. The CMSRs address fraud control issues such as personnel screening, separation of duties, rotation of duties, and training. Business partners should practice fraud control in accordance with the CMSRs and Appendix B, An Approach to Fraud Control.

3.10 Patch Management

(Rev. 11)

Timely patching is critical to maintaining the operational CIA of Medicare systems. However, failure to keep operating system and application software patched is the most common mistake made by IT professionals. New patches are released daily and it is often difficult for even experienced system administrators to keep abreast of all the new patches. The Computer Emergency Response Team (CERT)/Coordination Center (CC) (<http://www.cert.org>) estimates that 95 percent of all network intrusions could be avoided by keeping systems up-to-date with appropriate patches.

To help address this growing problem, CMS recommends that business partners have an explicit and documented patching and vulnerability policy and a systematic, accountable, and documented process for handling patches. The CMSRs provide specific guidance on time frames for implementing patches.

NIST SP 800-40 *Version 2.0*, Creating a Patch and Vulnerability Management Program, provides a valuable and definitive process for setting up, maintaining, and documenting a viable patch management process. CMS highly encourages business partners to utilize NIST and other guidance documents to develop configuration standards, templates, and management processes that securely configure Medicare systems as part of their configuration management program.

3.10.1 Security Configuration Management

(Rev. 10, Issued: 07-17-09, Effective: 08-17-09, Implementation: 08-17-09)

FISMA requires each agency to determine minimally acceptable system configuration requirements and ensure compliance with them. CMS security configuration management guidance, including CMS and DHHS requirements and links to NIST, National Security Agency (NSA), and Defense Information Systems Agency (DISA) configuration guides are provided in Appendix C, Security Configuration Management. CMS highly encourages business partners to utilize these and other guidance documents to develop configuration standards, templates, and processes that securely configure Medicare systems as part of their configuration management program.

CMS does not require the verbatim use of all security configuration guides and checklists for the configuration of Medicare systems. However, CMS does require that an active configuration management program be established and maintained, including the development/use of configuration standards within the entity. CMS also requires that entities include their “as designed/built” system security configuration with their GSS and/or MA SSPs.

Security configuration guidelines may be developed by different Federal agencies, so it is possible that a guideline could include configuration information that conflicts with another agency or CMS guideline. To resolve configuration conflicts among multiple security guidelines, the CMS hierarchy for implementing all security configuration guidelines is as follows:

1. CMS
2. DHHS
3. OMB
4. NIST
5. DISA

If there are any questions or concerns about resolving conflicts among security configuration guidelines, business partner SSOs shall contact their CMS Business Owner.

3.10.2 Security Technical Implementation Guides (STIG)

(Rev. 10, Issued: 07-17-09, Effective: 08-17-09, Implementation: 08-17-09)

Security guidelines, called STIGs, and security configuration checklists, called Checklists, are available for most major operating systems, support applications, and infrastructure services. STIGs contain detailed guidance, best practices, and recommendations for configuring a particular product. Checklists are a tool that provide detailed instructions for checking the presence of a vulnerability identified in a STIG. Both are developed by NSA, DISA, and NIST to help system operators configure security within their systems to the highest level possible. All STIGs and Checklists are available from DISA. The link for STIGs is: <http://iase.disa.mil/stigs/stig/index.html>, and the link for Checklists is: <http://iase.disa.mil/stigs/checklist/index.html>. CMS recommends that business partner SSOs (or their designated representative) subscribe to the DISA STIG-News Mailing List at: <http://iase.disa.mil/help/mailling-list.html> so they will be notified whenever updated or new STIGs become available.

The use of STIGs is mandatory for all business partner systems/applications that process, store, and/or transmit Medicare claims data. DMEMACs, ABMACs, and EDCs are required to start with the STIG baseline configurations and then document any exceptions based on environment specific implementation. While it may not be possible to implement all of a STIG's recommended security settings because doing so would compromise the functionality of an application and/or system, CMS expects every business partner to analyze the STIG recommended settings and determine which ones are feasible, and to implement all settings that are found to be feasible. All STIG recommended security settings that are determined not to be feasible in a business partner environment shall be documented in the applicable system/application IS RA with appropriate justification.

To assist business partners in implementing STIG security settings, there are several CMS Security Guides available for the more common systems/applications used in the business partner environment. These guides are available through the CMS IS "Virtual Handbook" Web site at: <http://www.cms.hhs.gov/InformationSecurity/>.

NSA has also developed and distributed configuration guidance for a wide variety of software from open-source to proprietary. The objective of the NSA configuration guidance program is to provide administrators with the best possible security options in the most widely used products. NSA provides these guidelines at: http://www.nsa.gov/snac/downloads_all.cfm.

The Center for Internet Security (CIS) provides security configuration benchmarks that represent a prudent level of due care, and are working to define consensus best-practice security configurations for computers connected to the Internet. CIS scoring tools analyze and report

system compliance with the technical control settings in the benchmarks. The CIS benchmarks and scoring tools are available for download at: <http://www.cisecurity.com/benchmarks.html>.

3.10.3 DHHS Federal Desktop Core Configuration (FDCC) Standard

(Rev. 10, Issued: 07-17-09, Effective: 08-17-09, Implementation: 08-17-09)

The DHHS is responsible for implementing and administering an information security and privacy program to protect its information resources. The DHHS must be compliant with applicable public laws, Federal regulations, and Executive Orders, including FISMA; OMB Circular A-130, Management of Federal Information Resources, and HIPAA. To meet these requirements, DHHS instituted the DHHS Information Security Program Policy and the DHHS Information Security Program Handbook documents.

The DHHS developed the DHHS FDCC Standard for Windows XP in response to OMB Memorandum (M)-07-11, Implementation of Commonly Accepted Security Configurations for Windows Operating Systems, released on March 22, 2007. In collaboration with its Operating Divisions (OPDIVs), DHHS developed the standard by testing the original FDCC standard provided by NIST on July 31, 2007, and making appropriate adjustments to best suit the DHHS and its OPDIV's environment. The resulting DHHS FDCC Standard must be implemented at each OPDIV (i.e., CMS) and its contractor computers that are owned or operated by a contractor on behalf of, or for, the OPDIV, or are integrated into a Federal system subject to FDCC.

The DHHS considers the DHHS FDCC Standard for Windows XP document "sensitive" so it is not publicly available. To obtain a copy of the DHHS FDCC Standard, the designated Systems Security Officer (SSO) from each business partner must request a copy via the CISS Help Desk (CISS@ngc.com). CMS expects business partners to request a copy and comply with the DHHS FDCC Standard for Windows XP.

3.10.4 National Institute of Standards and Technology (NIST)

(Rev. 10, Issued: 07-17-09, Effective: 08-17-09, Implementation: 08-17-09)

The Cyber Security Research and Development Act of 2002 (P.L. 107-305) tasks NIST to "develop, and revise as necessary, a checklist setting forth settings and option selections that minimize the security risks associated with each computer hardware or software system that is, or is likely to become widely used within the Federal government."

CMS, as a government agency, highly encourages business partners to review and incorporate the NIST concepts into their Medicare security program. Under the Computer Security Act of 1987 (P.L. 100-235), NIST develops computer security prototypes, tests, standards, and procedures to protect sensitive information from unauthorized access or modification. Focus

areas include cryptographic technology and applications, advanced authentication, public key infrastructure, internetworking security, criteria and assurance, and security management and support. These publications present the results of NIST studies, investigations, and research on IT security issues. The publications are issued as Federal Information Processing Standards (FIPS) Publications, Special Publications (SP), NIST Interagency Reports (NISTIRs), and IT Laboratory (ITL) Bulletins.

Special Publications in the 800 series (SP 800-xx) present documents of general interest to the computer security community. FIPS are issued by NIST after approval by the Secretary of Commerce pursuant to Section 5131 of the Information Technology Reform Act of 1996 (P.L. 104-106) and the Computer Security Act of 1987 (P.L. 100-235). With the passage of FISMA, there is no longer a statutory provision to allow for agencies to waive mandatory FIPS. The waiver provision had been included in the Computer Security Act of 1987; however, FISMA supersedes that Act. Therefore, any reference to a "waiver process" included in FIPS publications is no longer valid. Note, however, that not all FIPS are mandatory; consult the applicability section of each FIPS for details.

CMS does not normally require the verbatim use of NIST SPs for the configuration of Medicare systems. In cases where verbatim compliance is required, the requirements are specified in this BPSSM and the CMSRs. However, CMS highly encourages business partners to utilize NIST and other guidance documents to develop security standards, templates, and processes that securely configure Medicare systems as part of their configuration management program.

Table 3.4 contains a listing of NIST publications relevant to common systems or technology utilized within the Medicare business partner community. Table 3.4 is not meant to be all-inclusive and may contain some references that are not applicable to a particular Medicare business partner application. The most current NIST publications are available at: <http://csrc.nist.gov/publications/index.html>.

Table 3.4. NIST Publications

Publication Number	Title
SP 800-124	Guidelines on Cell Phone and PDA Security
SP 800-123	Guide to General Server Security
SP 800-121	Guide to Bluetooth Security
SP 800-115	Technical Guide to Information Security Testing and Assessment
SP 800-114	User's Guide to Securing External Devices for Telework and Remote Access
SP 800-113	Guide to SSL VPNs
SP 800-111	Guide to Storage Encryption Technologies for End User Devices
SP 800-110 (Draft)	Information System Security Reference Data Model
SP 800-106 (Draft)	Randomized Hashing Digital Signatures

Publication Number	Title
SP 800-103 (Draft)	An Ontology of Identity Credentials, Part I: Background and Formulation
SP 800-101	Guidelines on Cell Phone Forensics
SP 800-100	Information Security Handbook: A Guide for Managers
SP 800-98	Guidelines for Securing Radio Frequency Identification (RFID) Systems
SP 800-97	Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i
SP 800-96	Personal Identity Verification (PIV) Card to Reader Interoperability Guidelines
SP 800-95	Guide to Secure Web Services
SP 800-94	Guide to Intrusion Detection and Prevention Systems (IDPS)
SP 800-92	Guide to Computer Security Log Management
SP 800-89	Recommendation for Obtaining Assurances for Digital Signature Applications
SP 800-88	Guidelines for Media Sanitization
SP 800-86	Guide to Integrating Forensic Techniques into Incident Response
SP 800-85A	PIV Card Application and Middleware Interface Test Guidelines
SP 800-85B	PIV Data Model Conformance Test Guidelines
SP 800-84	Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities
SP 800-83	Guide to Malware Incident Prevention and Handling
SP 800-82 (Draft)	Guide to Industrial Control Systems (ICS) Security
SP 800-81	Secure Domain Name System (DNS) Deployment Guide
SP 800-80 (Draft)	Guide for Developing Performance Metrics for Information Security
SP 800-79-1	Guidelines for the Accreditation of PIV Card Issuers (PCIs)
SP 800-78-1	Cryptographic Algorithms and Key Sizes for PIV
SP 800-77	Guide to IPsec VPNs
SP 800-76-1	Biometric Data Specification for PIV
SP 800-73-2	Interfaces for PIV (4 parts): 1–End-Point PIV Card Application Namespace, Data Model, and Representation; 2–End-Point PIV Card Application Interface; 3–End-Point PIV Client Application Programming Interface; 4–The PIV Transitional Data Model and Interfaces
SP 800-72	Guidelines on PDA Forensics
SP 800-70 Rev. 1 (Draft)	Security Configuration Checklists Program for IT Products: Guidance for Checklists Users and Developers

Publication Number	Title
SP 800-69	Guidance for Securing Microsoft Windows XP Home Edition: A NIST Security Configuration Checklist
SP 800-68 Rev. 1 (Draft)	Guidance for Securing Microsoft Windows XP Systems for IT Professionals
SP 800-67-1.1	Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher
SP 800-66 Rev. 1	An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule
SP 800-65	Integrating IT Security into the Capital Planning and Investment Control Process
SP 800-64 Rev. 2	Security Considerations in the System Development Life Cycle
SP 800-63-1 (Draft)	Electronic Authentication Guidelines
SP 800-61 Rev. 1	Computer Security Incident Handling Guide
SP 800-60 Vol. 1	Guide for Mapping Types of Information and Information Systems to Security Categories
SP 800-60 Vol. 2	Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories
SP 800-59	Guideline for Identifying an Information System as a National Security System
SP 800-58	Security Considerations for Voice Over IP (VoIP) Systems
SP 800-57	Recommendation for Key Management
SP 800-56A	Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography
SP 800-55 Rev. 1	Performance Measurement Guide for Information Security
SP 800-54	Border Gateway Protocol Security
SP 800-53 Rev. 2	Recommended Security Controls for Federal Information Systems
SP 800-53A	Guide for Assessing the Security Controls in Federal Information Systems
SP 800-52	Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations
SP 800-51	Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme
SP 800-50	Building an IT Security Awareness and Training Program
SP 800-49	Federal S/MIME V3 Client Profile
SP 800-48 Rev. 1	Guide to Securing Legacy IEEE 802.11 Wireless Networks
SP 800-47	Security Guide for Interconnecting IT Systems
SP 800-46	Security for Telecommuting and Broadband Communications
SP 800-45 Ver. 2	Guidelines on Electronic Mail Security
SP 800-44 Ver. 2	Guidelines on Securing Public Web Servers

Publication Number	Title
SP 800-43	Systems Administration Guidance for Windows 2000 Professional System
SP 800-42	Replaced by SP 800-115
SP 800-41 Rev. 1 (Draft)	Guidelines on Firewalls and Firewall Policy
SP 800-40 Ver. 2	Creating a Patch and Vulnerability Management Program
SP 800-39 (Draft)	Managing Risk from Information Systems: An Organizational Perspective
SP 800-37 Rev. 1 (Draft)	Guide for Security Authorization of Federal Information Systems: A Security Lifecycle Approach
SP 800-36	Guide to Selecting IT Security Products
SP 800-35	Guide to IT Security Services
SP 800-34	Contingency Planning Guide for IT Systems
SP 800-33	Underlying Technical Models for IT Security
SP 800-32	Introduction to Public Key Technology and the Federal PKI Infrastructure
SP 800-30	Risk Management Guide for IT Systems
SP 800-29	A Comparison of the Security Requirements for Cryptographic Modules in FIPS 140-1 and FIPS 140-2
SP 800-28 Ver. 2	Guidelines on Active Content and Mobile Code
SP 800-27 Rev. A	Engineering Principles for IT Security (A Baseline for Achieving Security)
SP 800-25	Federal Agency Use of Public Key Technology for Digital Signatures and Authentication
SP 800-24	PBX Vulnerability Analysis: Finding Holes in Your PBX Before Someone Else Does
SP 800-23	Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products
SP 800-22	A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications
SP 800-21 2 nd Edition	Guideline for Implementing Cryptography in the Federal Government
SP 800-20	Modes of Operation Validation System for the Triple Data Encryption Algorithm (TMOVS): Requirements and Procedures
SP 800-19	Mobile Agent Security
SP 800-18 Rev. 1	Guide for Developing Security Plans for Federal IT Systems
SP 800-17	Modes of Operation Validation System (MOVS): Requirements and Procedures
SP 800-16	IT Security Training Requirements: A Role- and Performance-Based Model

Publication Number	Title
SP 800-15 Ver. 1	Minimum Interoperability Specification for PKI Components (MISPC)
SP 800-14	Generally Accepted Principles and Practices for Securing IT Systems
SP 800-13	Telecommunications Security Guidelines for Telecommunications Management Network
SP 800-12	An Introduction to Computer Security: The NIST Handbook
FIPS 201-1	PIV for Federal Employees and Contractors
FIPS 200	Minimum Security Requirements for Federal Information and Information Systems
FIPS 199	Standards for Security Categorization of Federal Information and Information Systems
FIPS 198-1	The Keyed-Hash Message Authentication Code (HMAC)
FIPS 197	Advanced Encryption Standard
FIPS 196	Entity Authentication Using Public Key Cryptography
FIPS 191	Guideline for the Analysis of Local Area Network Security
FIPS 190	Guideline for the Use of Advanced Authentication Technology Alternatives
FIPS 188	Standard Security Labels for Information Transfer
FIPS 186-3 (Draft)	Digital Signature Standard (DSS)
FIPS 186-3 Appendices (Draft)	RSA Strong Primers - DSS
FIPS 185	Escrowed Encryption Standard
FIPS 181	Automated Password Generator
FIPS 180-3 (Draft)	Secure Hash Standard (SHS)
FIPS 140-3 (Draft)	Security Requirements for Cryptographic Modules
FIPS 113	Computer Data Authentication

CMS continues to work closely with NIST in the development of new standards, FIPS, and security documentation to ensure the highest and most reasonable level of security of Medicare data.

3.11 Security Management Resources

3.11.1 Security Configuration Management

(Rev. 11)

FISMA requires each agency to determine minimally acceptable system configuration requirements and ensure compliance with them. CMS highly encourages business partners to

utilize guidance documents to develop configuration standards, templates, and processes that securely configure Medicare systems as part of their configuration management program.

Security configuration guidelines may be developed by different federal agencies, so it is possible that a guideline could include configuration information that conflicts with another agency or CMS guideline. To resolve configuration conflicts among multiple security guidelines, the CMS hierarchy for implementing all security configuration guidelines is as follows:

6. CMS
7. DHHS
8. OMB
9. NIST
10. DISA

(Note: DMEMACs, ABMACs, and EDCs are responsible for starting their security configurations with the DISA STIG Checklists)

If there are any questions or concerns about resolving conflicts among security configuration guidelines, business partner SSOs shall contact their CMS Business Owner.

3.11.2 Security Technical Implementation Guides (STIG)

(Rev. 11)

Security guidelines, called STIGs, and security configuration checklists, called Checklists, are available for most major operating systems, support applications, and infrastructure services. STIGs contain detailed guidance, best practices, and recommendations for configuring a particular product. Checklists are a tool that provide detailed instructions for checking the presence of a vulnerability identified in a STIG and configuring detailed system/application configuration settings. Both are developed by DISA to help system operators configure security within their systems to the highest level possible. All STIGs and Checklists are available from DISA. The link for STIGs and checklists is <http://iase.disa.mil/stigs/checklist/index.html>. CMS recommends that business partner SSOs (or their designated representative) subscribe to the DISA STIG-News Mailing List at: <http://iase.disa.mil/help/mailling-list.html> so they will be notified whenever updated or new STIG Checklists become available.

The use of latest publically available DISA STIG Checklists is mandatory for all business partner systems/applications that process, store, and/or transmit Medicare claims data. DMEMACs, ABMACs, and EDCs are required to start with the STIG baseline configurations and then

document any exceptions and/or deviations based on environment specific implementation. While it may not be possible to implement all of a STIG's recommended security settings because doing so would compromise the functionality of an application and/or system, CMS expects every business partner to analyze the STIG recommended settings and determine which ones are feasible, and to implement all settings that are found to be feasible. Settings that cannot be implemented on specific systems shall be documented as "system exceptions," and settings that cannot be implemented across an entire platform (e.g. Windows 2003, AIX) shall be documented as "system deviations." All STIG recommended security settings that are determined not to be feasible in a business partner environment shall be documented in the applicable system/application Security Configuration Checklist (SCC) with appropriate business justification (security impact, operational impact, business impact), mitigating or compensating controls, and residual risk.

Additional information is available through the CMS IS "Virtual Handbook" Web site at: <http://www.cms.hhs.gov/InformationSecurity/>.

3.11.3 DHHS Federal Desktop Core Configuration (FDCC) Standard

(Rev. 11)

The DHHS is responsible for implementing and administering an information security and privacy program to protect its information resources. The DHHS must be compliant with applicable public laws, Federal regulations, and Executive Orders, including FISMA; OMB Circular A-130, Management of Federal Information Resources, and HIPAA. To meet these requirements, DHHS instituted the DHHS Information Security Program Policy and the DHHS Information Security Program Handbook documents.

The DHHS developed applicable DHHS FDCC Standards for Windows in response to OMB Memorandum (M)-07-11, Implementation of Commonly Accepted Security Configurations for Windows Operating Systems. In collaboration with its Operating Divisions (OPDIVs), DHHS developed the standard by testing the original FDCC standard provided by NIST, and making appropriate adjustments to best suit the DHHS and its OPDIV's environment. The resulting DHHS FDCC Standards must be implemented at each OPDIV (i.e., CMS) and its contractor computers that are owned or operated by a contractor on behalf of, or for, the OPDIV, or are integrated into a Federal system subject to FDCC.

The DHHS considers the DHHS FDCC Standards for Windows documents "sensitive" so that they are not publicly available. To obtain a copy of the DHHS FDCC Standards, the designated Systems Security Officer (SSO) from each business partner must request a copy via the **CISO** Help Desk (CISO@cms.hhs.gov). CMS expects business partners to request copies and comply with the DHHS FDCC Standards for Windows.

3.11.4 National Institute of Standards and Technology (NIST)

(Rev. 11)

The Cyber Security Research and Development Act of 2002 (P.L. 107-305) tasks NIST to “develop, and revise as necessary, a checklist setting forth settings and option selections that minimize the security risks associated with each computer hardware or software system that is, or is likely to become widely used within the federal government.”

CMS, as a government agency, highly encourages business partners to review and incorporate the NIST concepts into their Medicare security program. Under the Computer Security Act of 1987 (P.L. 100-235), NIST develops computer security prototypes, tests, standards, and procedures to protect sensitive information from unauthorized access or modification. Focus areas include cryptographic technology and applications, advanced authentication, public key infrastructure, internetworking security, criteria and assurance, and security management and support. These publications present the results of NIST studies, investigations, and research on IT security issues. The publications are issued as Federal Information Processing Standards (FIPS) Publications, Special Publications (SP), NIST Interagency Reports (NISTIRs), and IT Laboratory (ITL) Bulletins.

Special Publications in the 800 series (SP 800-xx) present documents of general interest to the computer security community. FIPS are issued by NIST after approval by the Secretary of Commerce pursuant to Section 5131 of the Information Technology Reform Act of 1996 (P.L. 104-106) and the Computer Security Act of 1987 (P.L. 100-235). With the passage of FISMA, there is no longer a statutory provision to allow for agencies to waive mandatory FIPS. The waiver provision had been included in the Computer Security Act of 1987; however, FISMA supersedes that Act. Therefore, any reference to a "waiver process" included in FIPS publications is no longer valid. Note, however, that not all FIPS are mandatory; consult the applicability section of each FIPS for details.

CMS does not normally require the verbatim use of NIST SPs for the configuration of Medicare systems. In cases where verbatim compliance is required, the requirements are specified in this BPSSM and the CMSRs. However, CMS highly encourages business partners to utilize NIST and other guidance documents to develop security standards, templates, and processes that securely configure Medicare systems as part of their configuration management program.

The most current NIST publications are available at: <http://csrc.nist.gov/publications/index.html>.

CMS continues to work closely with NIST in the development of new standards, FIPS, and security documentation to ensure the highest and most reasonable level of security of Medicare data.

4 Information and Information Systems Security

4.1 Security Objectives

(Rev. 10, Issued: 07-17-09, Effective: 08-17-09, Implementation: 08-17-09)

FISMA defines three security objectives for information and information systems: confidentiality, integrity, and availability (CIA). FISMA also directs the promulgation of Federal standards for: (i) the security categorization of Federal information and information systems based on the objectives of providing appropriate levels of information security according to a range of risk levels; and (ii) minimum security requirements for information and information systems in each such category. These Federal standards are issued in the form of FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, and FIPS 200, Minimum Security Requirements for Federal Information and Information Systems, respectively.

4.1.1 Potential Security Impact Level

(Rev. 10, Issued: 07-17-09, Effective: 08-17-09, Implementation: 08-17-09)

FIPS 199 defines three levels of potential impact on organizations or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability). The application of these definitions shall take place within the context of each organization as it applies to the overall CMS mission objective.

Table 4.1 defines the three system security levels and their potential security impact.

Table 4.1. System Security Level Impact Definitions

Security Level	Result	Explanation
High (H)	Catastrophic Adverse Effect	<ul style="list-style-type: none">• Severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions;• Major damage to organizational assets;• Major financial loss; or• Severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

Security Level	Result	Explanation
Moderate (M)	Serious Adverse Effect	<ul style="list-style-type: none"> • Significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; • Significant damage to organizational assets; • Significant financial loss; or • Significant harm to individuals that does not involve loss of life or serious life threatening injuries.
Low (L)	Limited Adverse Effect	<ul style="list-style-type: none"> • Degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; • Minor damage to organizational assets; • Minor financial loss; or • Minor harm to individuals.

4.1.2 Security Level by Information Type

(Rev. 11)

Using FIPS 199, CMS categorized its information according to information type. An information type is a specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or, in some instances, by a specific law, Executive Order, directive, policy, or regulation.

CMS has defined *many* information types processed on and/or by CMS information systems. *These information types are defined in the CMS System Security and e-Authentication Assurance Levels by Information Type document, located at: <http://www.cms.gov/informationsecurity/downloads/ssl.pdf>.* For each information type, CMS used FIPS 199 to determine its associated security category by evaluating the potential impact value (e.g., High, Moderate, or Low) for each of the three FISMA security objectives—CIA. The resultant security categorization is the CMS System Security Level. This is the basis for assessing the risks to CMS operations and assets, and in selecting the appropriate minimum security controls and techniques (i.e., CMSRs).

4.1.3 CMS Security Level Designation—HIGH

(Rev. 11)

Although the confidentiality and integrity of some information types (i.e., security categorization [SC]) processed, stored, and/or transmitted on CMS business partner and data center systems could be considered to be at a “Moderate” security level based on the explanations and examples *in the CMS System Security and e-Authentication Assurance Levels by Information Type document*, CMS has designated all Medicare claims-related information to be “Mission-critical information.” Consequently, all CMS business partner and data center information systems shall be designated at a “HIGH” system security level.

Business partner system managers and system maintainers/developers shall ensure that their Medicare claims-related information and information systems are accessed only by authorized users. The business partner managers of compartmentalized systems shall take special care to specify the appropriate level of security required when negotiating with GSSs and MAs for services. The “HIGH” security level designation determines the minimum security safeguards (i.e., CMSRs) required to protect sensitive data and to ensure the operational continuity of mission-critical data processing capabilities.

The “HIGH” security level designation applies to both user information and system information, and it is applicable to information in both digital and non-digital form. System information (e.g., network routing tables, password files, and cryptographic key management information) shall be protected at the same level to ensure information and information system CIA.

4.1.4 Minimum System Security Requirements—HIGH

(Rev. 11)

FIPS 200 specifies minimum security requirements for information and information systems supporting the executive agencies of the federal government and a risk-based process for selecting the security controls necessary to satisfy the minimum security requirements. To comply with FIPS 200, agencies shall first determine the security category (i.e., information type) of their information system in accordance with the provisions of FIPS 199, and then apply the appropriate set of baseline security controls contained in NIST SP 800-53 *Rev. 3* (as amended), Recommended Security Controls for Federal Information Systems. Agencies have flexibility in applying the baseline security controls in accordance with the tailoring guidance provided in NIST SP 800-53 *Rev. 3*. This allows agencies, such as CMS, to adjust the security controls to more closely fit its mission requirements and operational environments.

The CMS Policy for the Information Security Program (PISP) individual policy statements, along with the CMS Minimum Security Requirements Procedure security standards provide

technical guidance to CMS and its contractors as to the minimum level of security controls that shall be implemented to protect CMS' information and information systems. These two CMS documents, along with other federal and CMS requirements, form the basis for the CMSRs.

4.2 Sensitive Information Protection Requirement

(Rev. 10, Issued: 07-17-09, Effective: 08-17-09, Implementation: 08-17-09)

Business partners are responsible for implementing the Minimum Protection Standards (MPS) for all CMS sensitive information (digital and non-digital) and information systems categorized at the "HIGH" security level designation. The MPS establishes a uniform method for protecting data and items that require safeguarding. The MPS applies to all IT facilities, areas, or systems processing, storing, or transmitting CMS sensitive information (i.e., any information categorized as "HIGH") in any form or on any media.

Care must be taken to deny unauthorized access to areas containing sensitive systems and information during working and non-working hours. This can be accomplished by creating restricted areas, security rooms, or locked rooms. Additionally, sensitive information in any form (computer printout, photocopies, tapes, notes, etc.) must be protected during non-duty hours. This can be done through a combination of methods: secured or locked perimeter, secured area, or containerization.

4.2.1 Restricted Area

(Rev. 10, Issued: 07-17-09, Effective: 08-17-09, Implementation: 08-17-09)

A restricted area is a secured area whose entry is restricted to authorized personnel (individuals assigned to the area). All restricted areas shall either meet secured area criteria or provisions shall be made to store CMS sensitive items in appropriate containers during non-working hours. The use of restricted areas is an effective method for eliminating unnecessary traffic through critical areas, thereby reducing the opportunity for unauthorized disclosure or theft of sensitive information. All of the following procedures must be implemented to qualify as a restricted area.

Restricted areas shall be indicated by prominently posted signs and separated from non-restricted areas by physical barriers that control access. The number of entrances should be kept to a minimum and each entrance shall have controlled access (e.g., electronic access control, key access, door monitor) to prevent unauthorized entry. The main entrance should be controlled by a responsible employee positioned at the entrance to enforce the restriction of access to authorized personnel accompanied by one or more officials.

When unescorted, a restricted area register shall be maintained at a designated entrance to the restricted area and all visitors (persons not assigned to the area) entering the area shall be directed to the designated entrance. Visitors entering the area shall enter (in ink) in the register: their name, signature, assigned work area, escort, purpose of entry, and time and date of entry.

The entry control monitor shall verify the identity of visitors by comparing the name and signature entered in the register with the name and signature of some type of photo identification card, such as a driver's license. When leaving the area, the entry control monitor or escort shall enter the visitor's time of departure. Each restricted area register shall be closed out at the end of each month and reviewed by the area supervisor/manager.

To facilitate the entry of employees who have a frequent and continuing need to enter a restricted area, but are not assigned to the area, an authorized access list (AAL) can be maintained. Each month a new AAL shall be posted and vendors shall be required to sign the register. If there is any doubt on the identity of the individual prior to permitting entry, their identity shall be verified prior to permitting entry.

4.2.2 Security Room

(Rev. 10, Issued: 07-17-09, Effective: 08-17-09, Implementation: 08-17-09)

A security room is a room that has been constructed to resist forced entry. The primary purpose of a security room is to store protectable material. The entire room shall be enclosed by slab-to-slab walls constructed of approved materials (e.g., masonry brick, dry wall, etc.) and supplemented by periodic inspection. All doors for entering the security room shall be locked with locking systems meeting the requirements set forth below (section 4.2.5, Locking Systems). Entry is limited to specifically authorized personnel.

Door hinge pins shall be non-removable or installed on the inside of the room. Any glass in doors or walls shall be security glass (a minimum of two layers of 1/8 inch plate glass with .060 inch [1/32] vinyl interlayer, nominal thickness shall be 5/16 inch). Plastic glazing material is not acceptable. Vents and louvers shall be protected by an Underwriters' Laboratory (UL)-approved electronic Intrusion Detection System (IDS) that annunciates at a protection console, UL-approved central station, or local police station; and the IDS shall be given top priority for guard/police response during any alarm situation.

Whenever cleaning and/or maintenance are performed, and sensitive systems and/or information may be accessible, the cleaning and/or maintenance shall be done in the presence of an authorized employee.

4.2.3 Secured Area (Secured Interior/Secured Perimeter)

(Rev. 10, Issued: 07-17-09, Effective: 08-17-09, Implementation: 08-17-09)

Secured areas are interior areas or exterior perimeters which have been designed to prevent undetected entry by unauthorized persons during working and non-working hours. Personnel may not reside in computer rooms and/or areas containing sensitive information unless that individual is authorized to access that sensitive information. To qualify as a secured area, the area shall meet the following minimum standards:

- Enclosed by slab-to-slab walls constructed of approved materials and supplemented by periodic inspection or other approved protection methods, or any lesser-type partition supplemented by UL-approved electronic IDS and fire detection systems.
- Unless electronic IDS devices are used, all doors entering the space shall be locked and strict key or combination control should be exercised.
- In the case of a fence/gate, the fence shall have IDS devices or be continually guarded, and the gate shall be either guarded or locked with intrusion alarms.
- The space shall be cleaned during working hours in the presence of a regularly assigned employee.

4.2.4 Container

4.2 - Sensitive Information Protection Requirements

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The term container includes all file cabinets (both vertical and lateral), safes, supply cabinets, open and closed shelving, desk and credenza drawers, carts, or any other piece of office equipment designed for the storage of files, documents, papers, or equipment. Some of these containers are designed for storage only and do not provide any protection value (e.g., open shelving). For purposes of providing protection, containers can be grouped into three general categories: locked containers, security containers, and safes or vaults.

4.2.4.1 Locked Container

(Rev. 10, Issued: 07-17-09, Effective: 08-17-09, Implementation: 08-17-09)

A locked container is a commercially available or prefabricated metal cabinet or box with riveted or welded seams, or metal desks with lockable drawers. The lock mechanism may be either a

built-in key, or a hasp and lock. A hasp is a hinged metal fastening attached to the cabinet, drawer, etc. that is held in place by a pin or padlock.

4.2.4.2 Security Container

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Security containers are metal containers that are lockable and have a tested resistance to penetration. To maintain the integrity of the security container, key locks should have only two keys and strict control of the keys is mandatory. If combinations are used, they shall be given only to those individuals who have a need to access the container. Security containers include the following:

- Metal lateral key lock files
- Metal lateral files equipped with lock bars on both sides and secured with security padlocks
- Metal pull drawer cabinets with center or off-center lock bars secured by security padlocks
- Key lock “Mini Safes” properly mounted with appropriate key control

If the central core of a security container lock is replaced with a non-security lock core, then the container no longer qualifies as a security container.

4.2.4.3 Safe/Vault

(Rev. 10, Issued: 07-17-09, Effective: 08-17-09, Implementation: 08-17-09)

A safe/vault is not required for storage of CMS sensitive information. However, if used, they shall meet the following requirements:

- A safe is a GSA-approved container of Class I, IV, or V, or UL listings of TRTL-30 or TRTL-60.
- A vault is a hardened room with typical construction of reinforced concrete floors, walls, and ceilings that uses UL-approved vault doors and meets GSA specifications.

4.2.5 Locking System

(Rev. 10, Issued: 07-17-09, Effective: 08-17-09, Implementation: 08-17-09)

The lock is the most accepted and widely used security device for protecting installations and activities, personnel data, sensitive data, classified material and government and personal property. All containers, rooms, buildings, and facilities containing vulnerable or sensitive items shall be locked when not in actual use. However, regardless of their quality or cost, locks should be considered as delay devices only and not complete deterrents. Therefore, locking system must be planned and used in conjunction with other security measures.

Minimum requirements for locking systems for secured areas and security rooms are high-security pin-tumbler cylinder locks that meet the following requirements:

- Key-operated mortised or rim-mounted deadbolt lock
- Have a deadbolt throw of one inch or longer
- Double-cylinder design; cylinders have five or more pin tumblers
- Contains hardened inserts or inserts made of steel if bolt is visible when locked
- Both the key and lock shall be “off-master”

Convenience-type locking devices such as card keys, sequenced button-activated locks used in conjunction with electric strikes, etc., are authorized for use only during working hours. Keys to secured areas not in the personal custody of an authorized employee and any combinations shall be stored in a security container. The number of keys or persons with knowledge of the combination to a secured area shall be kept to a minimum.

4.2.6 Intrusion Detection System (IDS)

(Rev. 10, Issued: 07-17-09, Effective: 08-17-09, Implementation: 08-17-09)

Physical IDSs are designed to detect attempted breaches of perimeter areas. Physical IDS devices can be used in conjunction with other measures to provide forced entry protection for non-working hour security. Additionally, alarms for individual and document safety (fire), and other physical hazards (water pipe breaks) are recommended. Alarms shall annunciate at an on-site protection console, a central station, or local police station. Physical IDS devices include, but are not limited to: door and window contacts, magnetic switches, motion detectors, and sound detectors, that are designed to set off an alarm at a given location when the sensor is disturbed.

4.2.7 Minimum Protection Alternatives

(Rev. 11)

The objective of the MPS is to prevent unauthorized access to CMS sensitive information. MPS requires two barriers to accessing sensitive information under normal security. The reason for the two barriers is to provide an additional layer of protection to deter, delay, or detect surreptitious entry. Because local factors may require additional security measures, management shall analyze local circumstances to determine space, container, and other security needs at individual facilities.

Table 4.1 shall be used to determine the minimum protection alternatives required to protect CMS sensitive information. Note that any of the three alternative protection standards is acceptable whenever all of the applicable perimeter, interior area, and/or container standards are met. The protection alternative methods are not listed in any order of preference or security significance.

Table 4.1. Protection Alternative Chart

	Perimeter Type	Interior Area Type	Container Type
Alternative #1	Secured		Locked
Alternative #2	Locked	Secured	
Alternative #3	Locked		Security

4.3 Encryption Requirements for Data Leaving Data Centers

(Rev. 11)

CMS, as a trusted custodian of individual health care data, must protect its most valuable assets—its information and its information systems. Consequently, CMS believes that putting the government's credibility at risk is not acceptable.

Effective immediately, and until further notice, no data that includes personally identifiable information (PII) shall be transported from a CMS data center (including business partner data centers and subcontractor data centers) unless it has been encrypted. The encryption requirement may only be waived through written concurrence from the Business Owner of the data followed by a "wet" signature from the CMS CIO, Deputy CIO, or the Chief Technology Officer (CTO).

The **only** exception to this requirement is for tapes destined for off-site storage or for the purpose of data center transitions, and that data must be shipped using proper precautions (i.e., locked in sturdy containers).

This protected health information (PHI) data protection requirement, published in CIO Directive 07-01 dated June 12, 2007, is in accordance with:

- CMS Policy for the Information Security Program (PISP) section *4.1.10, Media Protection: Information system media, both digital and non-digital must be protected by: (i) limiting access to information on information system media to authorized users; and (ii) sanitizing or destroying information system media before disposal or release for reuse.*
- CMS Minimum Security Requirements (CMSRs):
 - MP-5: All sensitive information stored on digital media are protected during transport outside of controlled areas by using cryptography and tamper proof packaging and (a) if hand carried, using securable container (e.g., locked briefcase) via authorized personnel, or (b) if shipped, trackable with receipt by commercial carrier. If the use of cryptography is not technically feasible or the sensitive information is stored on non-digital media, written management approval (one level below the CIO) must be obtained prior to transport and the information must be (a) hand carried using securable container via authorized personnel, or (b) if shipped, by United States Postal Service (USPS) Certified Mail with return receipt in tamper-proof packaging. Correspondence pertaining to a single individual may be mailed through regular USPS mail, but should contain the minimal amount of sensitive information in order to reduce the risk of unauthorized disclosure.
 - MP-5(2): Activities associated with the transport of sensitive information system media are documented.
 - MP-5(3): For systems designated at a "HIGH" sensitivity level, employ an identified custodian at all times to transport information system media.

5 Internet Security

(Rev. 11)

With prior written approval of their sponsoring CMS Business Owner, business partners may now use Internet technology for transmission of and/or receipt of health care transactions. Each request for using Internet technology will be considered individually and approval is not automatic. However, any approval shall require that business partners meet CMS architectural, security, data interchange, and privacy requirements for Internet-facing infrastructure. Further, an independent (third-party) *Security Control Assessment* of the new functionality prior to its

release into production is required and the *Security Control Assessment* must include penetration testing. The *Security Control Assessment* is conducted to validate compliance with the following specific architectural, security, data interchange, and privacy requirements, as well as the CMSRs. The *Security Control Assessment* must be conducted by a CMS-contracted third party. The existing requirement for an annual penetration test of the contractor network shall include any approved Internet infrastructure. Compliance with existing requirements to conduct quarterly vulnerability scans and annual penetration testing is still mandatory.

Briefly, architectural, security, data interchange and privacy requirements include the following:

1. Architecture:

- Explicit compliance with CMS system lifecycle standards, particularly:
 - CMS Technical Reference Architecture, Version 1.0, and all its appendices, and
 - CMS Java EE Application Development Guidelines.
- Utilization of resources to leverage existing technology and solutions such as platform and software developed by contractors and in compliance with CMS standards to meet the same or similar business requirements. The technology and solutions would also have to align with requirements for the Medicare Administrative Contractors, Enterprise Data Centers, and Standard Front End initiatives.

2. Security:

- Full compliance with the CMS Integrated IT Investment & System Life Cycle Framework (Checkpoints, Deliverables, and Activities including *Security Authorization*) in introducing the new functionality.
- Satisfactory systems test and evaluation of the Internet application to include evaluation of all 17 control categories set forth in the CMSRs.
- Compliance with DHHS and CMS standard configuration settings.
- Compliance with the NIST SP 800-41 *Rev. 1*, Guidelines on Firewalls and Firewall Policy; NIST SP 800-44 *Version 2*, Guidelines on Securing Public Web Servers; and NIST SP 800-115, Technical Guide to Information Security Testing and Assessment.
- *Security Authorization* dependent on compliance with security control requirements and completion of documentation such as the IS RA, the IS SSP for the infrastructure, platform, and applications supporting the Internet functionality, and a CP for the supporting platform and application. The IS RA must address e-authentication requirements and controls for electronic transactions, or refer to a separate document if one exists. All security documentation must be developed to the CMS methodologies and procedures provided at: http://www.cms.hhs.gov/InformationSecurity/14_Standards.asp#.

3. Privacy: Completion of a Privacy Impact Assessment (PIA) as set forth in Section 208 of the E-Government Act.

4. Data Interchange:

- Utilization of HIPAA compliance standards for applicable transactions (i.e. claims, remittances and inquiry/response for eligibility and claim status) to be enabled by the new functionality.
- Enabling both batch file transfer and interactive screen presentation for the HIPAA transactions.
- 508 compliance for interactive screen presentation.
- All Internet and non-Internet data exchange modes (i.e. Interactive Voice Recognition, Direct Data Entry, and Computer to Computer) shall return consistent data.
- Compliance with Trading Partner authentication requirements including submitter/provider relationship for the HIPAA transactions.

Application requirements include but are not limited to the following:

1. A proof of concept/concept of operation paper describing the new application and functionality.
2. Information that the Internet service shall be extended only to entities or providers enrolled in the jurisdiction of the proposing business partner.
3. An attestation that the applicant has had a similar private-side application that has been in production for more than one year. The attestation shall describe the experience of the private-side application and how it relates to the Internet proposal.

Other application requirements may be imposed by the sponsoring CMS business component.

Additionally, business partners may also use the Internet for: 1) utilizing the IRS Filing Information Returns Electronically (FIRE) system for Form 1099 submissions, and 2) utilizing e-mail to transmit sensitive information via encrypted attachments in accordance with all applicable CMSRs. An application for these uses is not required. If not already emplaced, contractors must install firewalls, filtering technology to screen incoming *e-mail* for high risk transmissions such as executables, up-to-date virus protection software, and intrusion detection software to utilize the *I*nternet for these purposes.

Appendix A: Medicare Information Technology (IT) Systems Contingency Planning

(Rev. 10, Issued: 07-17-09, Effective: 08-17-09, Implementation: 08-17-09)

Table of Contents

- 1 Introduction**
- 2 Scope**
- 3 Definition of an Acceptable Contingency Plan**
- 4 Medicare IT Systems Contingency Planning**
 - 4.1 Contingency Planning
 - 4.2 Coordination with Other Business Partners
- 5 Medicare IT Systems Contingency Plan**
- 6 Testing**
 - 6.1 Claims Processing Data Centers
 - 6.2 Multiple Contractors
 - 6.3 Test Types
 - 6.3.1 Live vs. Walkthrough
 - 6.3.2 End-to-End
 - 6.4 Local Processing Environments (PCs/LANs)
 - 6.5 Test Planning
- 7 Minimum Recovery Times**
- 8 Responsibilities**
 - 8.1 Business Partner Management
 - 8.2 Systems Security Officer (SSO)
 - 8.3 Service Components (provide support functions such as maintenance, physical security)
 - 8.4 Operating Components (IT operations personnel)
- 9 Changes**

- 10 Attachments**
- 11 Checklist**
- 12 References**

1 Introduction

(Rev. 10, Issued: 07-17-09, Effective: 08-17-09, Implementation: 08-17-09)

CMS business partners are required by CMS Minimum Security Requirement (CMSR) security control Contingency Planning-1 (CP-1) to develop and maintain a Contingency Plan (CP). This plan is to provide information to aid the business partner in planning for and responding to an emergency or system disruption, and to recover from that emergency or disruption.

Section 3.4 of the BPSSM requires that all CMS Medicare business partners prepare, review, and test their Medicare IT Systems Contingency Plans. All general support systems (GSS) and major applications (MA) that support critical Medicare operations shall be covered by a Medicare IT Systems Contingency Plan (CP).

This document presents the direction for accomplishing Medicare IT systems contingency planning. It is to be used by the CMS Medicare business partner management, IT systems management and staff, and system security persons charged with preparing for continuing the operation of Medicare systems and developing an IT systems CP, or updating an existing plan.

The business partner information security risk assessment may be used as a checkpoint to determine if appropriate contingencies have been addressed in the CP.

To ensure the CP is workable, it shall be thoroughly and periodically tested.

The simplified diagram in Figure A-1 illustrates the IT systems contingency planning process.

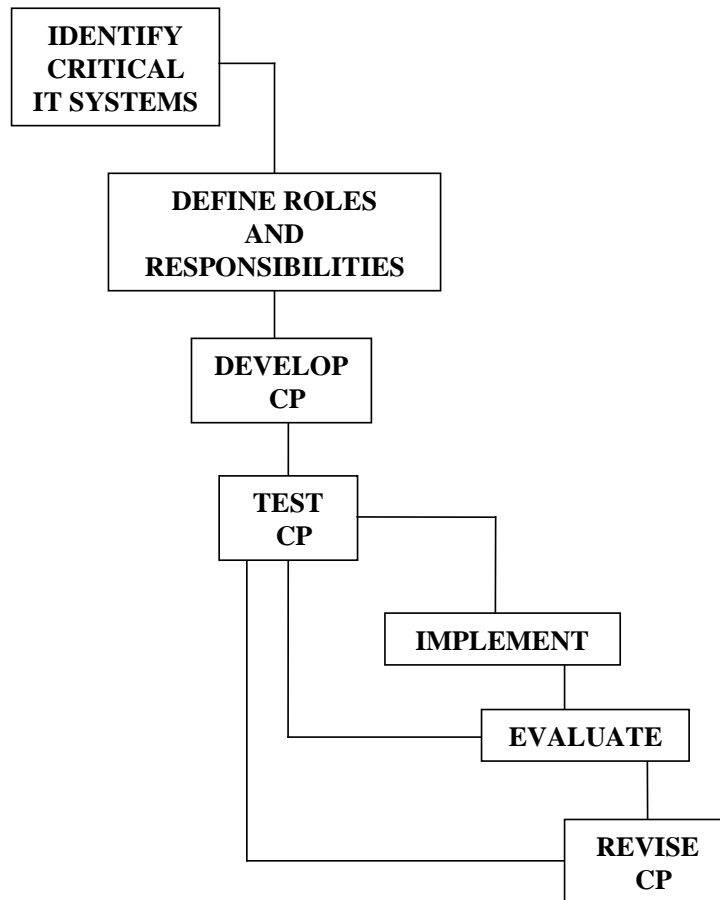


Figure A-1 – IT Systems Contingency Planning Process

2 Scope

(Rev. 10, Issued: 07-17-09, Effective: 08-17-09, Implementation: 08-17-09)

The business partner IT systems CPs address organizations and sites where Medicare data is processed, including claims processing locations, data centers, and other processing or printing sites.

3 Definition of an Acceptable Contingency Plan

(Rev. 10, Issued: 07-17-09, Effective: 08-17-09, Implementation: 08-17-09)

A CP is a document that describes how to plan for and deal with an emergency or system disruption. These situations could be caused by a power outage, hardware failure, fire, or terrorist

activity. A CP is developed and maintained to ensure quick, appropriate, effective, and efficient response in those situations for which a foreseen risk cannot be mitigated or avoided.

Protecting lives is the paramount task while executing a CP.

Before developing an IT systems CP, it is advisable to have or create a contingency policy. The CP shall be driven by a contingency policy. The contingency policy is a high level statement relative to what the management wants to do to address a contingency and to recover from the emergency or system disruption.

The IT systems CP shall be developed under the guidance of IT management and systems security persons and all organizational components shall be actively involved in providing information for developing the plan, for making plan related decisions, and for providing support to plan testing.

It can be a very subjective argument relative to what constitutes an acceptable CP. In this document, the description of an acceptable CP is based on the results of the research, analysis and review of various documents from Government and industry, and the review of existing business partner CPs and test reports.

The following summary statements define what constitutes an acceptable CP. This is not an all-inclusive list and the topics are not in any order of importance or priority.

1. Considers the protection of human life as the paramount guiding principle, and then aims at the backup, recovery, and restoration of critical business functions, protecting equipment and data, and preserving the business reputation for providing high-quality service.
2. Is logical, reasonable, understandable, user friendly, and can be implemented under adverse circumstances.
3. Considers risk assessment results.
4. Addresses possible and probable emergencies or system disruptions.
5. Can be sufficiently tested on an established regular basis at reasonable cost.
6. Contains information that is needed and useful during an emergency or system disruption.
7. Can, when implemented, produce a response and recovery, such that critical business functions are continued.

8. Specifies the persons necessary to implement the plan, and clearly defines their responsibilities.
9. Clearly defines the resources necessary to implement the plan.
10. Reflects what can be done – is not a wish list.
11. Assumes people shall use sound judgment, but will need clearly stated guidance, since they will be functioning in a non-normal environment, under possibly severe pressure.
12. Addresses backup and alternate sites.
13. Addresses the use of manual operations, where appropriate and necessary.
14. Contains definitive “Call Lists” to use for contacting the appropriate persons in the proper sequence. This list would include vendor points of contact.

An acceptable CP should be straight to the point. It should not contain any more information than is necessary to plan for and implement contingency actions. The users should not get bogged down in detail as they read the plan to determine what to do, when to do it, what is needed to do it, and who should do it. The CP should serve as a “user’s manual” and be easy to understand and use.

Because a CP is designed to be used in a stressful situation, it shall be written with that as a foremost thought in mind. The prime objective is to maximize the continuity of critical operations.

Reviewing a CP and testing it will help determine whether it remains an acceptable plan. The review and testing shall not focus solely on content, but shall also focus on ease of use.

A complete set of CPs for an organization may be made up of several smaller CPs, one for each business function (e.g. claims processing) or for a single data center, for example. This breakdown into manageable parts helps to keep a plan easy to use.

Careful thought should be given to the organization of the CP. The organization should be logical in terms of what will the user want to know or do first. If the first thing that should happen in an emergency is that a call list shall be used to notify persons, then that call list, or a pointer to it, should be placed very near the front of the CP. Not every informational item to be utilized during a contingency event will be in the CP document. For example, the plan may point to an attachment or to a separate procedures manual. In this regard, a CP should contain a very understandable and useful table of contents, so that a user can quickly find the information being sought.

Contingency planning can provide a cost-effective way to ensure that critical IT capabilities can be recovered quickly after an emergency. IT systems contingency planning shall embrace a coordinated contingency policy of what will be done to fully recover and reconstitute all operations.

4 Medicare IT Systems Contingency Planning

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

The goal of IT systems contingency planning is to continue accomplishing critical Medicare IT systems operations in an emergency or system disruption and to accomplish a rapid and smooth recovery process.

4.1 Contingency Planning

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Contingency planning is preparing for actions in the event of an emergency situation, and giving some thought and planning to what your organization will do to respond and recover. The IT systems contingency planning process shall address all the actions and resources needed to ensure continuity of operation of critical Medicare IT systems and the means of implementing the needed resources. IT management and staff shall be trained to handle emergency or system disruption situations in data centers and other areas where data processing systems are located. Contingency planning includes such training.

It is advisable to establish a Medicare IT systems contingency planning team. This team would be responsible for defining critical Medicare IT systems, including applications software, data, processing and communications capabilities, and other supporting resources. These would be the key people in the implementation of the plan.

4.2 Coordination with Other Business Partners

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

If a business partner's data center or other data processing environment is linked to other business partners for the transmission of Medicare data, then the contingency planning shall include those links relative to receiving input, exchanging files, and distributing output. If alternate/backup IT systems capabilities are to be utilized, then their functions and data transmission links shall be considered in the planning.

Coordination with other business partners is essential to completing the IT systems contingency planning process.

5 Medicare IT Systems Contingency Plan

(Rev. 10, Issued: 07-17-09, Effective: 08-17-09, Implementation: 08-17-09)

The following format may be used in developing a Medicare IT Systems CP. While this format is not required, all of its elements shall be included in the CP.

1. Introduction
 - Background
 - Purpose/Objective
 - Management commitment statement
 - Scope
 - Organizations
 - Systems
 - Boundaries
 - IT capabilities and resources
 - CP policy
 - Priorities
 - Continuous operation
 - Recovery after short interruption
 - Minimum recovery times
2. Assumptions
3. Authority/References
4. Definition of what the CP addresses
 - Organizations
 - Systems
 - Boundaries
5. Three phases defined
 - Respond
 - Recover
 - Restore/reconstitute
6. Roles/Responsibilities defined
7. Definition of critical functions
8. Alternate capabilities and backup
9. Definition of required resources to respond and recover

10. Training

- CP shall address Who – When – How

11. Testing the CP

- Philosophy
- Plans
- Boundaries
- Live vs. Walkthrough
- Reports
- Responsibilities

12. CP maintenance/updating

- Schedule

13. Relationships/Interfaces

- Outside (vendors, providers, banks, utilities, services, CMS)
- Internal
- Dependencies

14. Attachments

- Actions for each phase
- Procedures
- Call trees
- Vendor contact list
- Hardware inventory
- Software inventory
- System descriptions
- Alternate/Backup site information
- Assets/Resources
- Risk Assessment Summary (refer to System Security Plans)
- Agreements/Memos of Understanding
- Manual Operations
- Supplies/Materials/Equipment
- Floor plans
- Maps

The CP shall provide for off-site storage:

- Backup software
- Data
- Appropriate documents (emergency telephone lists, memos of understanding, etc.)
- Copies of the CP

- Administrative supplies (forms, blank check stock, etc.)

6 Testing

(Rev. 10, Issued: 07-17-09, Effective: 08-17-09, Implementation: 08-17-09)

CMS requires testing of the CP annually under conditions that simulate an emergency or a disaster. A CP shall also be tested after a substantive system change that necessitates a revision to the CP.

CMS requires that the critical IT systems shall be tested annually and the CP updated to accommodate any changes, including updated versions of software or critical data. Critical systems are those whose failure to function, for even a short time, could have a severe impact, or have a high potential for fraud, waste, or abuse.

6.1 Claims Processing Data Centers

(Rev. 10, Issued: 07-17-09, Effective: 08-17-09, Implementation: 08-17-09)

Many of the contractors with which CMS has direct contracts do not have their own data centers. They usually contract this service out. If a business partner does not have its own data center, then it is the responsibility of the business partner to inform the subcontractor that operates the data center that they shall have a CP.

6.2 Multiple Contractors

(Rev. 10, Issued: 07-17-09, Effective: 08-17-09, Implementation: 08-17-09)

Data centers usually serve multiple contractors. Existing shared processing environments allow for multiple contractors to process claims at a data center. There are numerous data centers processing Part A and Part B claims for multiple Medicare contractors.

It is important to test a CP at a data center that serves multiple contractors. This provides a mechanism to examine the possible commingling of data between contractors, wherein data may be compromised.

Before testing of the CP begins, it is important to understand how contractor data is protected and/or kept separate. The data centers may use a security package, such as ACF, to control access and separation of data. In order to perform appropriate testing, the complexity of the data center operation must be understood.

6.3 Test Types

(Rev. 10, Issued: 07-17-09, Effective: 08-17-09, Implementation: 08-17-09)

CP test guidance suggests four types of testing:

- Walkthrough
- Simulation/modeling
- Tabletop Test
- Live

These are defined below:

- **Walkthrough:** A walkthrough test is accomplished by going through a set of steps to accomplish a particular task or action initiated because of a contingency event. The precursor to a walkthrough test is that the steps are documented so that they can be logically followed. A “test team” might sit around a table and talk through each step and then walk through” the various steps, and then discuss expected outcomes and further actions to be taken. They may use a checklist to ensure that all features of a step are addressed or that all resources necessary to accomplish the task or action are considered. A walkthrough test does not involve accomplishing the actions being tested in real time or using the live environment. A walkthrough test could be accomplished by using a group of test people to act out what might happen if a real contingency event occurred. They might go to the alternate site, but they would not actually start all hardware, software, and communication operations in order to assume the function of the primary site.
- **Simulation/Modeling:** Modeling involves creating a computer model of the process to be tested. This allows easy testing of many variables without physically having to make changes. For example, you can vary the number of servers that go down during a disaster or the number of people that can get to an alternate site following a disaster.

Simulation involves taking physical actions, but not necessarily to the full extent of what might actually happen during an emergency. For example, instead of actually moving everyone to an alternate site to continue operations, a small team may undertake a set of realistic preparatory actions at the prime site, and another team does the same at the alternate site. Thus, many steps could be simulated by the two teams and worthwhile results evaluated.

- **Tabletop Test:** For those applications that are both hosted at CMS and not participating in a broader recovery test to a CMS-approved recovery site during their annual test cycle, a tabletop test is required. A tabletop test is discussion-based only, and does not involve

deploying equipment or other resources. The discussion during the test can be based on a single scenario or multiple scenarios. By simulating an emergency in an informal, stress-free environment, this test method allows for the free exchange of ideas and provides participants an opportunity to practice the steps to be followed in an actual event and to identify areas in the CP for enhancement..

A successful tabletop test steps participants through real-life scenarios; captures its results in a formal report; and incorporates the “lessons learned” into subsequent versions of the CP and the tabletop test plan. Refer to CMS Contingency Planning Tabletop Test Procedures, for step-by-step instructions for conduction a tabletop test.

- **Live:** This is the most complete and expensive test to accomplish. It involves completing the physical steps that would actually be taken if an emergency occurred. People and materials would be moved to an alternate site for the test, and servers would actually be shut down to reduce capability. Power would be shut off, and live conditions would be tested. A live test uses actual environments, people, and components to accomplish the test in real time. It is the real thing, nothing artificial, or made up, is substituted. If the test is to see if an alternate site capability can be implemented, then in a live test, the hardware, software, data, communications, and people at the alternate site would be set into action and begin functioning as the primary site to support operations.

End-to-end refers to the scope of the testing (partial testing is less than end-to-end). When conducting end-to-end testing, items to consider include:

- End-to-end testing can be completed as part of walkthrough or live test.
- Not testing end-to-end means that some links, processes, or subsystems are missed.
- What is the risk in not conducting end-to-end testing?
- Live end-to-end testing can be very expensive!

Considering risks and cost, management shall make a decision as to what type and scope of testing is appropriate.

6.3.1 Live vs. Walkthrough

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

- High-level testing can take the form of a walkthrough test.
- A walkthrough can be part of the overall testing process, but not the whole process.

- Lower-level testing can include a walkthrough, if live testing is not an option.
 - Live testing shall be the first choice.
 - Fall back to a simulation/model if live testing is not an option.
Cost, time, and interruption of normal operations are major considerations in doing a live test.
 - A walkthrough test should be the last resort.
- Ask what a walkthrough test would miss.
- Consider the ramifications of missing that part of the test.
- Remember that there is risk in not doing a live test—can the risk be accepted?
 - Consider the criticality of functions, processes, and systems.
If critical to continuing essential business operations, then these are strong candidates for live testing.
- Testing interfaces.
It is important to test the critical interfaces with internal and external systems. It is difficult to test interfaces using a “walkthrough” method. Simulation or “live” testing is preferred.
- Cost and complexity.
The decision as to how to test critical functions, processes, and systems must result from careful consideration of complexity and cost. A complete “live” test of all elements of an operation may prove to be extremely costly, in terms of both dollars and time. If that cost out weighs the “cost” of the risk of not doing live testing, then “live” testing should probably be ruled out.

6.3.2 End-to-End

(Rev. 10, Issued: 07-17-09, Effective: 08-17-09, Implementation: 08-17-09)

This kind of testing aims to ensure that all software and hardware components associated with a function, process, or system are tested from the front end through to the back end (input through process through output). As with live testing, end-to-end testing can be expensive.

- End-to-end testing shall only be considered for critical functions, processes, or systems.
- Why is end-to-end testing needed?
It provides the best assurance that there are no problems.

- Would a partial test be meaningful?
If the overall process to be tested can be sub-divided into critical and non-critical components, then only the critical ones need be considered for end-to-end testing.
- Examples of types of end-to-end tests:
 - Claims receipt through to check generation
 - Query of a database through to the response
 - Medicare Secondary Payer (MSP) check request through to check issue and back to MSP
- Evaluate complexity and cost.
The decision on how to test critical functions, processes, and systems shall carefully consider complexity and cost. A complete end-to-end test of all elements of an operation may prove to be extremely costly, both in terms of dollars and time. If that cost outweighs the cost of the risk of not doing end-to-end testing, then end-to-end testing should probably be ruled out.
- Consider the criticality of functions, processes, and systems.
Look at the criticality of functions, processes, and systems. If these are critical to continuing essential business operations, then these are strong candidates for end-to-end testing.
- If you cannot do end-to-end testing, then consider live testing of all links possible to help ensure minimum problems.
 - Or, do simulation/modeling
 - Or, do walkthrough

Overall testing may take the form of reviews, analyses, or simulations of contingencies. Reviews and analyses may be used for non-critical systems, whereas critical systems shall be tested under conditions that simulate an emergency or a disaster.

It is advisable that the testing of critical systems be done end-to-end, input through output, so that no physical activity, automated process, or Medicare business partner system is left untested. Critical interfaces internal and external to the systems shall be tested.

Testing may include activities in addition to computer processing. Manual operations shall be checked according to procedures, and changes made as experience indicates.

6.4 Local Processing Environments (PCs/LANs)

(Rev. 10, Issued: 07-17-09, Effective: 08-17-09, Implementation: 08-17-09)

IT systems CP testing relative to local environments, such as individual or clustered workstations and local area network (LAN) configurations, may be less comprehensive than data center testing. Reviews and analyses may be used to accomplish certain non-critical systems testing, whereas critical systems require full simulation or live testing. The criticality of the system is the deciding factor relative to what type testing is used, how often tests are accomplished, and how thorough the testing shall be.

The decision of which test approach to use relative to a specific system or configuration shall be a management decision based on advice from the System Security Officer (SSO), IT systems staff, operations and support representatives, and the lead test planner/manager.

6.5 Test Planning

(Rev. 10, Issued: 07-17-09, Effective: 08-17-09, Implementation: 08-17-09)

An IT systems contingency test plan shall address at least the following:

- Test objectives
- Test approach
- Required equipment and resources
- Necessary personnel
- Schedules and locations
- Test procedures
- Test results
- Failed tests
- Corrective action management process
- Retest
- Approvals

It is advisable to establish test teams responsible for preparing and executing the IT systems CP tests. Responsibilities shall be assigned to test team members, including executives, observers, and contractors.

Following testing, the corrections specified in a Corrective Action Management Process shall be tested. The process shall include:

- List of items that failed the previous test
- Corrections planned

- Retest detail
- Schedule
- Review responsibilities

Ensure that the lessons learned from IT systems CP testing are discussed among senior business partner management, operations, IT management and staff, and the SSO.

Documentation shall exist for:

- Test plans
- Test results
- Corrective action management process
- Retest plans
- Memos of Understanding/Formal Test Arrangements

7 Minimum Recovery Times

Recovery time is the time it takes to recover an operation, function, process, program, file, or whatever has to be recovered as an operational entity.

Minimum recovery time is the longest acceptable period of time for recovery of operations. If claims processing operations must be recovered within 72 hours, then that is the minimum acceptable time to recover. Anything over that is unacceptable.

- Recovery times shall vary, depending on the criticality of the entity involved.
- Times can be from a few minutes to days or weeks.
- A table/matrix can be constructed that lists the recovery times.
- There can be a separate table/matrix for each organization or major function (e.g., claims processing, medical review, check generation).
- Recovery times shall be carefully defined and must be achievable.
- Recovery times can be verified to some extent through testing (simulation or live).

8 Responsibilities

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

Following is a summary of responsibilities for key groups and persons involved with contingency planning.

8.1 Business Partner Management

(Rev. 10, Issued: 07-17-09, Effective: 08-17-09, Implementation: 08-17-09)

- Defines scope and purpose of IT systems contingency planning.
- Authorizes preliminary IT systems contingency planning.
- Ensures that appropriate CPs are developed, periodically tested, and maintained.
- Ensures that all IT operations participate in the contingency planning and the development of the plans.
- Reviews the plan and recommendations.
- Requests and/or provides funds for plan development and approved recommendations.
- Assigns teams to accomplish development of test procedures, and for testing the plan.
- Reviews test results.
- Ensures that the appropriate personnel have been delegated the responsibility for effecting backup operations, and that the backup copies of critical data are ready for use in the event of a disruption.
- Ensures that the business partner organization can demonstrate the ability to provide continuity of critical IT systems operation in the event of an emergency.
- Business partner management shall approve:
 - The CP
 - Changes to the CP
 - Test Plans
 - Test results
 - Corrective action management processes
 - Retest Plans
 - Memos of Understanding/Formal Arrangement Documents
 - Changes to storage and backup/alternate site facilities

8.2 Systems Security Officer (SSO)

(Rev. 10, Issued: 07-17-09, Effective: 08-17-09, Implementation: 08-17-09)

- Documents the scope and purpose of IT systems contingency planning
- Reconciles discrepancies and conflicts
- Evaluates security of backup and alternate sites
- Leads the preparation of the CP
- Submits the plan and recommendations to management
- Monitors implementation of the plan and reports status to management
- Ensures all testing of the plan is accomplished as required
- Reviews test results
- Ensures that the plan is updated based on test results

8.3 Service Components (provide support functions such as maintenance, physical security)

(Rev. 9, Issued: 06-20-08, Effective: 07-01-08, Implementation: 07-22-08)

- Maintain physical security forces to respond to emergencies.
- Schedule fire and other emergency drills and monitor effectiveness.
- Develop emergency re-supply procedures for forms, supplies, equipment, and furniture.
- Provide for priority replacement of computer hardware.
- Provide for restoring telecommunications.
- Provide for backup sites and procedures.
- Provide information relative to the availability of recovery sites.
- Develop procedures for documenting inventories of equipment and furniture.
- Provide a list of employees' home addresses and phone numbers.
- Support testing of the plan.

8.4 Operating Components (IT operations personnel)

(Rev. 10, Issued: 07-17-09, Effective: 08-17-09, Implementation: 08-17-09)

- Designate employees for emergency response teams.
- Designate employees for backup teams.
- Designate employees for recovery teams.
- Provide a list of employees' home addresses and phone numbers.
- Identify time-critical operations and systems.

- Identify critical resources, such as hardware, software, data, communications, facilities, and people.
- Identify supplies (forms, blank check stock, etc.) to be stored at alternate sites.
- Identify critical data to be backed up offsite.
- Provide information on testing requirements.
- Accomplish and/or support end-to-end system testing.
- Review test results.
- Identify critical, non-automated data processing operations.
- Review basic service organization plans and advise SSO where needs are not met.
- Monitor CP implementation and report status to management.

9 Changes

(Rev. 10, Issued: 07-17-09, Effective: 08-17-09, Implementation: 08-17-09)

The CP shall be updated whenever one or more of the following events occurs:

- New systems or operations added.
- Upgrade or replacement of Standard System software.
- Hardware or software replacement.
- Changed back up/alternate site.
- Changed storage facilities.
- Removal of existing systems or operations.

10 Attachments

(Rev. 10, Issued: 07-17-09, Effective: 08-17-09, Implementation: 08-17-09)

Materials that are too extensive to be included in the body of the Medicare IT Systems CP shall be included as attachments. These shall be referenced in the contingency plan. These shall also be a part of the System Security Profile. Existing material that facilitates response, backup, and recovery operations shall be included as attachments or a pointer provided. Much of this material is bulky and relates to the entire organization. The SSO shall ensure that the information to be attached is pertinent and current, and that updated copies are routinely incorporated, particularly into offsite copies of the CP. Such material includes:

- Master inventories of forms, supplies, and equipment
- Description of computer hardware and peripherals
- Description of applications software
- Appropriate security weakness information
- Systems and program documentation

- Prioritized schedules for computer operations
- Communications requirements, especially computer networks

11 Checklist

(Rev. 10, Issued: 07-17-09, Effective: 08-17-09, Implementation: 08-17-09)

The following checklist provides a means for determining if a CP contains the appropriate information that can readily be used in handling an emergency or system disruption. This list is not all-inclusive, but rather should serve as a thought stimulus for evaluating CPs.

This checklist uses the same outline as the suggested CP format.

1. Introduction

Does the CP contain:

- Background
Is a history of the plan provided? Are the physical environment and the systems discussed?
- Purpose/Objective
What does the plan address? Why was it written? What does it aim to accomplish?
- Management Commitment Statement
Has the CP been approved by management and the SSO? Once the CP is created, reviewed, and ready for distribution, it shall be approved by site, operations and information systems management, and the SSO.
- Scope
Are the boundaries of the plan indicated? What organizations are involved, not involved?
 - Organizations
 - Systems
 - Boundaries
- IT Capabilities and Resources
Is the focus of the plan on IT systems, capabilities, and resources?
- CP Policy
 - Priorities
 - Are the CP steps ranked according to priority?

- Continuous Operation
 - Are there functions, processes, or systems that are required to continue without interruption?
 - Recovery after Short Interruption
 - Which functions, processes, or systems can be interrupted for a short time?
 - Recovery Times?
 - Are the recover times stated?
 - What are the minimum recovery times?
 - Standalone Units
 - Does a CP exist for any standalone workstation? A key part of a CP shall address any standalone workstations that are part of the critical operations environment. It shall state where backup software and support data for these workstations is stored.
 - Is the plan reviewed and approved by other key affected persons?
2. Assumptions
Are all the important assumptions listed? Have the assumptions been carefully reviewed by the appropriate persons to ensure their validity?
3. Authority/References
- Who or what document is authorizing the creation of the CP?
 - What are the key references that apply to the plan?
4. Definition of what the CP Addresses
- Organizations
To which organizations does the CP apply?
 - Systems
Is there a general description of systems and/or processes?
 - Boundaries
Are the system boundaries clearly defined?
5. Three phases defined
Does the plan address three phases of emergency or system disruption?
- Respond

- Is this phase adequately described so that it is understood what activities occur therein?
- Is damage/impact assessment considered?
- Are the alerting and initial impact assessment procedures fully explained as well as arrangements for continual review of their use and effectiveness?
- Recover
Is this phase adequately described so that it is understood what activities occur during this phase?
- Restore/Reconstitute
Is this phase adequately described so that it is understood what activities occur during this phase?

6. Roles/Responsibilities Defined

- Has the necessary CP implementation organization been defined and the responsibilities of all those involved clearly stated with no 'gray areas'?
- Will all who have a task to perform be aware of what is expected of them?
- Does the CP assign responsibilities for recovery? The responsibilities of key management and staff persons shall be carefully described in the CP, so that there is no question relative to the duties of these people during an emergency.

7. Definition of Critical Functions

- Does the CP address critical systems and processes?
- Have emergency processing priorities been established and approved by management?
- Does the CP specify critical data? The CP shall specify the critical data needed to continue critical business functions and how frequently the data is backed up.
- Has a list of critical operations, data, and applications been created? In preparation for preparing the CP, a list of current critical operations, data and applications shall be prepared and approved by management. This list shall contain the items needed to continue the critical business functions until operations could be returned to a normal mode.

8. Alternate Capabilities and Backup

- Have arrangements been made for alternate data processing and telecommunications facilities? Part of contingency planning includes the completion of arrangements for alternate data processing facilities and capabilities, and for alternate telecommunications capabilities necessary to re-establish critical interfaces.
- Does the CP address issues relative to pre-planned alternate locations? The CP shall address any potential issues relative to pre-planned alternate locations. These include:
 - insurance
 - equipment replacement
 - phones
 - utilities
 - security
- Does contingency backup planning exist? Planning for appropriate backup of data and processing capabilities shall include:
 - prioritizing operations
 - identifying key personnel and how to reach them
 - listing backup systems and where they are located
 - stocking critical forms, blank check stock, and supplies off-site
 - developing reliable sources for replacing equipment on an emergency basis
- Is there an alternate information processing site; if so, is there a contract or interagency agreement in place?
- Are the levels of equipment, materials and manpower sufficient to deal with the anticipated emergency? If not, have back-up resources been identified and, where necessary, have agreements for obtaining their use been established?
- Have temporary data storage sites and location of stored backups been identified?
- Is the frequency of file backup documented?
- Have the arrangements been made for ensuring continuing communications capabilities?
- Are backup files created on a prescribed basis and rotated off-site often enough to avoid disruption if current files are damaged?
- Are system, application, and other key documentation maintained at the off-site location?
- Are the backup storage and alternate sites geographically removed from the primary site and physically protected?

- Do data and program backup procedures exist? In order to be prepared for an emergency, it is advisable to provide backups of critical data and software programs. These are stored at off-site locations sufficiently distant from the primary site so as not to be affected by the same emergency that would affect the primary site.
- Is the CP stored off-site at alternate/backup locations? Copies of the CP shall be stored at several off-site locations, including key personnel homes, so that at least one copy is readily available in time of emergency. Copies of the CP that are stored in a private home shall be protected from inadvertent access.

9. Required Resources

- Are the following resources for supporting critical operations defined and available for an emergency?
 - Hardware
 - Software
 - Communications
 - Data
 - Documents
 - Facilities
 - People
 - Supplies
 - Basic essentials (water, food, shelter, transportation, etc.)
- Does the CP provide for backup personnel? As the CP is implemented, it is necessary to have additional people available to support recovery operations. The CP shall specify who these people are and when they would normally be called into action.

10. Training

- Are management and staff trained to respond to emergencies? Security training shall include modules for management and staff relative to their roles for handling emergency situations.

11. Testing the CP

- Is there a section in the CP that addresses testing of the plan?
- Testing of the CP shall address the following topics:
 - Test Philosophy
 - Test Plans
 - Boundaries
 - Live vs. Walkthrough vs. End-to-End Testing

- Test Reports
- Responsibilities

12. CP Maintenance

- Schedule
 - Is the CP annually reviewed and tested? The CP shall be reviewed and tested annually under conditions as close to an emergency as can be reasonably and economically simulated.
 - Is there a provision for updating the CP annually?
 - Is the CP revised after testing, depending on test results?

13. Relationships/Interfaces

- Does the CP identify critical interfaces? Interfaces required to continue critical business functions should be identified. Refer to the System Security Plans.
- Which outside (vendors, providers, banks, utilities, services, CMS) interfaces must be considered?
- Is the plan compatible with plans of interacting organizations and systems?
- What internal interfaces must be considered?
- Is the plan compatible with plans of interacting organizations and systems?
- Which corporate interfaces must be considered?
- Are there special interfaces with corporate systems that must be addressed in the CP?

14. Attachments

Does the CP contain appropriate attachments, as listed below?

A. Actions for Each Phase

Are the actions to be taken in each phase (respond, recover, restore) of the contingency clearly described and related to organizations and/or people?

B. Procedures

- Are there detailed instructions for:
 - responding to emergencies?

- recovering?
- restoring operations?
- Do contingency backup agreements exist? Agreements with organizations or companies which will provide service, equipment, personnel, or facilities during an emergency shall be in place.
- Are there procedures for addressing the situation where the processing site is intact, but people can't get to it because of a natural disaster? Can the business be operated remotely?
- Is there an implementation plan for working from home?

C. Call Trees

Are there call lists with names, addresses, and phone numbers with priority order relative to whom to call first?

D. Hardware Inventory

Are there lists of all the hardware covered by the CP?

E. Software Inventory

Are there lists of all the software covered by the CP?

F. System Descriptions

Are all the systems covered by the CP defined, including appropriate diagrams?

G. Alternate/Backup Site Information

Is there sufficient detail to completely describe the alternate and/or backup sites, including addresses, phone numbers, contacts, resources available at the sites, and, resources needed to be brought to the site?

H. Assets/Resources

Are there lists of all the needed resources for responding, recovery, and restoring operations?

I. Risk Assessment Summary

Has there been a realistic assessment of the nature and size of the possible threat and of the resources most at risk?

J. Agreements/Memo of Understanding

Are there agreements in place relative to the use of alternate/backup sites, special resources, outside suppliers, extra people, alternate communications, etc?

K. Manual Operations

Are manual operating procedures in place so that certain functions can continue manually if automated support is not available soon enough?

Manual processing procedures shall exist in the backup phase until automated capabilities can take over the information processing. Provisions shall be made to provide this manual capability.

L. Supplies/Materials/Equipment

Is there information that describes how and where to obtain needed supplies, materials, and equipment?

M. Floor Plans

Are the necessary floor plans available?

N. Maps

Are the necessary area and street maps available?

12 References

(Rev. 11, Issued: 09-30-11, Effective: 10-31-11, Implementation: 10-31-11)

In addition to this manual, the following documents may be referenced during the IT systems contingency planning process:

- NIST Special Publication 800-34 *Rev. 1*, Contingency Planning Guide for Information Technology Systems, *May 2010*.
<http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1.pdf>

- NIST Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook, Chapter 11.
<http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf>
- Health Insurance Portability & Accountability Act (HIPAA): The Race to Become Compliant, Ed Deveau, Disaster Recovery Journal, Fall 2000.
- Federal Information System Controls Audit Manual (FISCAM), Exposure Draft, GAO-08-1029G, Section 3.5.
<http://www.gao.gov/new.items/d081029g.pdf>
- Presidential Decision Directive/NSC 63 (PDD 63), White Paper: The Clinton Administration's Policy on Critical Infrastructure Protection, May 22, 1998.
http://www.usdoj.gov/criminal/cybercrime/white_pr.htm
- OMB Circular No. A-123, Management's Responsibility for Internal Control, Revised, December 21, 2004.
http://www.whitehouse.gov/omb/circulars/a123/a123_rev.html
- Office of Management & Budget, Circular No. A-130, Appendix III, Security of Federal Automated Information Resources, 8 February 1996.
http://www.whitehouse.gov/omb/circulars/a130/a130appendix_iii.html
- CMS Contingency Planning Tabletop Test Procedures, Version 1.1., 25 July 2007.
http://www.cms.hhs.gov/informationsecurity/downloads/cp_tabletop_template.zip

Appendix B: An Approach to Fraud Control

(Rev. 10, Issued: 07-17-09, Effective: 08-17-09, Implementation: 08-17-09)

Table of Contents

- 1 Introduction**
- 2 Safeguards against Employee Fraud**
- 3 Checklist for Medicare Fraud**

1 Introduction

(Rev. 8, Issued: 04-06-07; Effective Date: 10-01-06; Implementation Date: 05-01-07)

This document develops countermeasures relating to fraudulent acts and a checklist to help Medicare contractors assess their vulnerability to fraud. Fraud and embezzlement are skyrocketing, largely because basic safeguards are neglected or lacking. Fraudulent acts are discussed in terms of the types of safeguards in place and functioning.

2 Safeguards against Employee Fraud

(Rev. 10, Issued: 07-17-09, Effective: 08-17-09, Implementation: 08-17-09)

The following safeguards are specific countermeasures against fraudulent acts by employees whose functions involve Medicare program funds. These safeguards are consistent with the CMS Information Security Acceptable Risk Safeguards (ARS) Including CMS Minimum Security Requirements (CMSRs) outlined in Appendices A, B, and C; and do not constitute wholly different or additional minimum requirements. The following countermeasures should prove especially effective against currently prevalent fraudulent activities and are discussed primarily as they relate to prevention and detection of fraud.

A. Screen New Employees

Screen new employees for positions that involve program funds directly or indirectly to address the applicant's past faithful and honest performance of duties with other employers in addition to job performance and investigation of his/her personal finances. New employees' statements concerning personal finances shall be confirmed with former employers and with banking and credit institutions. Phone calls to previous employers are

essential, particularly to former supervisors who should be advised of the nature of the position. Although former employers will sometimes fail to prosecute employees associated with fraudulent activities, they seldom delude a prospective employer asking about the applicant's integrity.

Any blatant dishonesty in the application (such as claiming qualifications and experience the applicant never had) shall remove the applicant from further consideration. Check references and crosscheck them (one against the other) for consistency as well as content. Evaluate references on the basis of the contact's personal knowledge of the applicant's job-related qualifications and integrity.

Proper screening is preventive medicine at its best. Gaps in employment are flags that call for third-party verification, not just a plausible explanation by the applicant. Former employers may be able to shed light on the situation or be able to relate the reason given them about gaps by the applicant.

Circumstances relating to termination of previous employment should be clearly related by former employers. Resolve any inconsistencies or vagueness.

Ask former employers as well as the applicant, whether the employee was ever bonded, or was ever refused bonding. Sensitive screening should not result in violating an applicant's civil rights, while assuring you (and your bonding company) that prudent concern is exercised in the hiring process.

B. Bonding

Bonding is also known as fidelity insurance and comes in all configurations; the broader the coverage, the more expensive the premium. One of the most important things you can do is analyze the extent and conditions of coverage in relation to possible misappropriations of funds. Liability is invariably limited in some respects. For example, coverage often does not extend to external fraud; to losses not proven to have been caused by fraudulent acts by covered employees; to frauds committed by employees known to have perpetrated dishonest acts previously; to frauds whose circumstances are not properly investigated; or to frauds whose alleged perpetrators are not brought to trial. Inherent in the analysis of bonding is risk analysis of fraud in relation to specific components to develop a worst-case fraud scenario in terms of dollar-loss before recovery through bonding.

C. Separation of Duties

Separate duties so that no one employee can defraud the company unaided. This is the cardinal rule for fraud prevention, one that is well-understood in manual operations. It is not as well understood in its application to computer processing where a single automated system may combine functions ordinarily separated, such as transactions and

adjustments. Analyze all duties, including all stages of computer programming and operations, in terms of defeating single-handed fraud as well as in terms of effectiveness and efficiency, with fraud controls taking precedence. Group review of programmer code before allowing new/upgraded systems into production is the type of duty-separation (function vs. approval) that serves both effectiveness and security.

D. Rotation of Duties

Rotate duties, particularly those involving authorization of a transaction. Separation of duties makes it difficult for an employee to defraud your organization unaided, so that embezzlement becomes a crime of collusion. As more and more embezzlement involves more than one person, it becomes necessary to ensure that the same person is not always involved in approving another's functions. An employee is less likely to initiate a fraudulent transaction if he/she is not certain that his/her accomplice will be the one to approve or process that transaction. Moreover, the knowledge that from time to time other employees will perform his/her function or work his/her cases is a powerful deterrent to any fraudulent scheme, particularly embezzlement which requires continual cover-up.

E. Manual Controls

Manual controls are differentiated from automatic controls because constant review is necessary to see that they are in place and working. Moreover, they often supplement or augment automatic controls; for example, the manual review of claims rejected in computer processing. Review all manual controls to determine the extent to which they would be effective against fraud in any operational area; too often, controls are reviewed without fraud specifically in mind. Classic manual controls are those associated with the tape/disk library, and these controls are strongly associated with restricted access and separation of duties. It does little good to separate programmer/operator duties if the programmer is allowed to sign out production tapes or master files for any reason, especially live-testing. Library controls shall require specific authorization for tape removal for specific periods for specific reasons known to, and sanctioned by, the approving authority. The most important manual controls are those over blank-check stock and the automatic check-signer. The employee in control of the check-signer shall not at the same time control the check stock, although these duties may be rotated so that the person controlling the check-signer one day may be assigned to control check stock on the following day when a third person is responsible for the check-signer. However, no one individual shall be allowed to "sign" a check he/she has issued. Rotation of duties is proper only for subsequent operations where one's own previous actions have already cleared.

F. Training

Training employees in their responsibilities relative to fraud in their operations is basic to prudent management. This extends beyond the employee's own activities. For example, Title 18, U.S. Code Section 4 requires anyone having knowledge of a Federal crime to report it to the Federal Bureau of Investigation (FBI) or similar authority, with penalties of up to \$500 fine and 3 years in jail for failure to do so. No employee should be ignorant of this responsibility. This responsibility can be explained as a simple good citizenship requirement and not spying or snitching. Discuss these things periodically in meetings, along with free give-and-take on moral issues and management's position on every aspect of fraud, including perpetration involving collusion with outsiders. Do not single out any employee or function in these discussions, instead make management's position clear regarding so-called "justification" for unauthorized "borrowing" and the fact that fraud can and will be prosecuted. Explain that there can be no permissive attitude towards dishonest acts because such an attitude is corrupting and makes it difficult for employees to remain honest. Make it known that there are controls throughout the organization to prevent and detect fraud, without being specific as to how they work. Require employees to report apparent loopholes in security that might one day (or already) be exploited for fraudulent purposes. Remind employees that ethical conduct requires their full cooperation in the event of any fraud investigation, and when interviewed they shall be called upon to explain why security gaps or suspicious activities were not reported to the SSO. No security program can be effective without the involvement and cooperation of employees, and nowhere is this truer than with fraudulent activity.

G. Notices

Notices, both periodic and situational, are effective and necessary in the prevention and control of fraud. It is not enough to formulate management policy or to conduct employee training relative to fraudulent activity. It is possible to remind employees of management's continuing concerns and to evaluate employee awareness through simple reminders or announcements of what is happening relative to fraud controls (of a general nature) and management's reliance on their cooperation and understanding of their responsibilities. Without this evidence of sustained management commitment, policy utterances tend to fade from memory or become regarded as part of a new employee's orientation and not part of the scene. This is true of minor abuses, but is also true of abuses that escalate into fraud.

H. Automatic Controls

Automatic controls to prevent or detect fraudulent activities comprise the first line of defense in computer operations. Such controls are often thought of as ensuring data integrity but more in terms of accuracy than of honesty. Evaluate automatic controls in terms of preventing payment to unauthorized persons. Test automatic controls with

fraudulent (invalid) input, under strict control of courses, and with management's full cognizance and prior approval.

I. Audit Routines

Audit routines are those programs where trained auditors test for fraud using special routines to reveal computer processing that creates or diverts payments to employees or their accomplices. Wrongdoers not only have to create bogus payments, but also they have to be able to lay their hands on the checks in order to cash them. Devise audit routines to single-out payments being directed to post office boxes or to repeat addresses (where such repeats would be unreasonable), to the addresses of an employee or his family, or to a drop-off address that is not a real business but merely a place to collect mail.

3 Checklist for Medicare Fraud

(Rev. 10, Issued: 07-17-09, Effective: 08-17-09, Implementation: 08-17-09)

This checklist represents questions to address in analyzing the security of Medicare fiscal operations.

- 1) Have Medicare operations been identified where fraud or complicity in fraud may be possible, e.g. initiation/approval of payments?
- 2) Have individuals been assigned fraud-protection responsibilities in such components, including the responsibility for reporting possible fraud and vulnerability to fraud?
- 3) Do individual employees at all levels understand that management policy relative to fraud is dismissal and prosecution?
- 4) Are fiscal operations regularly audited relative to fraud vulnerability?
- 5) Are fraudulent acts specifically mentioned in the employee's code of ethical conduct?
- 6) Is employee integrity specifically addressed during the hiring process, and do background investigations elicit information that would uncover an applicant's past fraudulent activity with other employers?
- 7) Are operations set up in such a way as to discourage both individual and collusive fraudulent activity?
- 8) Are programs/systems tested by authorized individuals with "fraudulent" input?

- 9) Are audit trails generated that identify employees who create inputs or make adjustments/corrections that would pinpoint responsibility for any fraudulent act?
- 10) Is there an effective mechanism for detection/prevention of payments being purposely misdirected to employees, relatives, or accomplices?
- 11) Are new or changed programs specifically reviewed for fraudulent code by those responsible for production-run approval (persons empowered to review changes but not to make changes themselves)?
- 12) Are controls designed to prevent fraud, especially in those operations where large sums could be embezzled quickly?
- 13) Are all error-conditions checked for fraud potential?
- 14) Are balancing operations done creatively so that an embezzler could not hide discrepancies?
- 15) Are the official activities of all employees, at all levels, subject to independent review by different reviewers (i.e., not always by the same evaluator)?
- 16) Does management insist on integrity at all levels?
- 17) Has management announced that employee's work activities will be reviewed (in unspecified ways) for both the fact and appearance of integrity?
- 18) Do tape/disk library controls in fact prevent tampering with files/programs for fraudulent purposes?
- 19) Are alternative fraud controls invoked during emergencies?
- 20) Are suspected frauds investigated promptly and properly and are they thoroughly documented?
- 21) Are fraud audits conducted both periodically and randomly?
- 22) Are random samples taken of claims/bill inputs and checked back to their sources?
- 23) Does the Personnel Department check the applicant's background, employment record, references, and possible criminal record before hiring?
- 24) Are badges, identification cards/numbers, and passwords promptly issued and rescinded?

- 25) Is off-hours work supervised, monitored, or otherwise effectively controlled?
- 26) Are all employees required to take their vacations and are their replacements required to check over the vacationers' past activities?
- 27) Are the credentials of outsiders, such as consultants and auditors, checked out?
- 28) Is temporary help bonded, hired from reputable agencies, and their activities restricted to the tasks to be performed? (Same principle applies to employees temporarily borrowed from non-Medicare components.)
- 29) Are written procedures controlled and restricted to employees currently assigned the relevant duties?
- 30) Are special fraud controls specified for backup operations?
- 31) Are incoming checks, including returned checks, handled by two or more individuals in the mailroom and are such teams switched around so that the same people are not always working together?
- 32) Are blank checks and automatic check-signing equipment strictly controlled with a tamper-proof numbering mechanism?
- 33) Is procedure/program documentation relative to the payment process treated as highly sensitive data and safeguarded when superseded?
- 34) Are backup files current and securely stored off-site?
- 35) Are re-runs checked for the possibility of fraud, especially duplicate payments?

Transmittals Issued for this Chapter

Rev #	Issue Date	Subject	Impl Date	CR#
<u>R11SS</u>	09/30/2011	CMS Business Partners System Security Manual	10/31/2011	7328
<u>R10SS</u>	07/17/2009	Business Partners System Security Manual	08/17/2009	6410
<u>R9SS</u>	06/20/2008	CMS Business Partners System Security Manual	07/22/2008	5976
<u>R8SS</u>	04/06/2007	CMS Business Partners System Security Manual	05/01/2007	5500
<u>R7SS</u>	03/17/2006	Self Assessment process in Appendix A and Core Security Requirements	05/01/2006	4342
<u>R6SS</u>	12/09/2005	Incorporation of JSM Instructions in sections 1 through 3	01/09/2006	4111
<u>R5SSS</u>	12/23/2004	Miscellaneous Changes in sections 1 through 3	02/28/2005	3605
<u>R4SSM</u>	03/05/2004	Update links, expand on security concepts, clarify core security requirements and security activities to be conducted/followed, include due dates for system security activities and minor editorial changes.	04/05/2004	3106
<u>R3SSM</u>	03/28/2003	Miscellaneous corrections and clarifications in 1-5 and Appendices	04/11/2003	2568
<u>R2SSM</u>	02/13/2002	Replacement of Manual	02/13/2002	2015
<u>R1SSM</u>	03/28/2003	Initial Issuance of Manual	01/26/2001	1439