Centers for Medicare & Medicaid Services (CMS)

Business Partners

Systems Security Manual

CENTERS FOR MEDICARE & MEDICAID SERVICES

7500 SECURITY BOULEVARD

BALTIMORE, MD 21244-1850

(Rev. 15.1, Issued:07-17-25)

CMS/ Business Partners
Systems Security Manual

Record of Changes

(Rev. 15.1; Issued: 07-17-25; Effective: 02-28-25; Implementation: 08-18-25)

Revision	Major Changes	Date
12	Main Document and all Appendices (1) Updated Internet hyperlinks throughout document (2) Changed "EISG" (Enterprise Information Security Group) to "ISPG" (Information Security and Privacy Group" throughout document (3) Correct typographical errors	08/2013
13	Main Document and all Appendices (1) Deleted Section 3.6.1/Computer Security Incident Response due to duplication (2) Added Section 3.12/End Of Life Technology Components (3) Added Section 3.13/Cloud Computing (4) Added Attachment 1/MAC ARS	06/2017
14	Main Document and all Appendices (1) Updated ARS references to MAC ARS (2) Added section 3.14/MAC ARS Control Tailoring (3) Added section 3.15/Data Loss Prevention (4) Added section 3.16/Wireless Access Monitoring (5) Added section 3.17/ Malicious Software (6) Added section 3.18/Whitelisting (7) Added section 3.19/Data Encryption (8) Updated Attachment 1/MAC ARS	02/2018
15	Multiple changes have been made to the document (1) Late addition: Added Section 3.9 on Identity Proofing (2) Updated various sections and language throughout	05/2022
15.1	*Multiple changes have been made to the document* *(1) Updated Internet hyperlinks throughout the document* *(2) Changed CMS Virtual Data Centers (VDC) to Third Party Data Centers (TPDC)* *(3) Updated various sections and language throughout* *(4) Updated Attachment 1/MAC ARS*	*11/2024*

CMS/Business Partners
Systems Security Manual

Table of Contents

(Rev. 15.1; Issued: 07-17-25; Effective: 02-28-25; Implementation: 08-18-25)

Table of Contents

Appendices

Appendix A Medicare Information Technology (IT) Systems Contingency Planning

Appendix B An Approach to Fraud Control

Attachments

Attachment 1 Medicare Administrative Contractor Acceptable Risk Safeguards

1 - Introduction

(Rev. 15.1; Issued: 07-17-25; Effective: 02-28-25; Implementation: 08-18-25)

Key Requirements
This manual addresses the following key Medicare Fee-For-Service *(FFS)* business partner security elements:

- A business partner is a contractor involved in Medicare *FFS* claims processing
- 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 can be found on the CMS Information Security Web site at: *https://security.cms.gov*
- The specific version of the ARS to be used by the Medicare Administrative Contractors (MAC) is the MAC ARS, which is Attachment A of this document
- MACs *shall implement the ARS High Value Asset (HVA)* controls *contained within the MAC ARS*

The Centers for Medicare and Medicaid Services (CMS) provides health coverage to more than 100 million people through Medicare, Medicaid, the Children's Health Insurance Program, and the Health Insurance Marketplace. As a Federal agency, the systems used to process data are required to follow the Federal Information Security Modernization Act (FISMA) of 2014.

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 Federal Information Processing Standards (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.

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.

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., MAC Acceptable Risk Safeguards [ARS] controls).

Federal Information Processing Standards (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 the current version of NIST SP 800-53. 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. This allows agencies, such as CMS, to adjust the security controls to more closely fit its mission requirements and operational environments.

The CMS Information Security and Privacy Policy contains individual policy statements, along with the CMS Minimum Security Requirements, 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, are used to form the basis for the CMS ARS.

The "Medicare Prescription Drug, Improvement, and Modernization Act of 2003 (MMA) - Section 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 (MAC)," 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. In addition, the term ARS is used in this manual to mean the ARS that includes the required security and privacy control baselines and tailored with the supplemental controls identified by the Business Owner and Information System Security Officer (ISSO). For the MACs, this will be known as the MAC ARS.

CMS requires that the MACs, the primary CMS Medicare claims processing business partner, implement information security controls on their information technology (IT) systems to maintain the CIA of Medicare systems operations in the event of computer incidents or physical disasters.

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 supported by senior management and staffed by individuals with proper training and knowledge.

1.1 - Additional Requirements for MACs

(Rev. 15.1; Issued: 07-17-25; Effective: 02-28-25; Implementation: 08-18-25)

MACs are responsible for fulfilling all existing business partner requirements. Additional requirements include the following:

- The contractor shall comply with the CMS MAC tailored list of controls found in Attachment 1. This list of controls, known as the MAC ARS, includes all of the CMS required controls plus optional controls are included specifically for the MACs. MAC ARS controls will be tailored via the BPSSM as what is included in the BPSSM overrides the MAC ARS controls with the intent of being more restrictive.

- The contractor shall correct weaknesses, findings, gaps, or other deficiencies within 90 days of receipt of any final audit or evaluation report *regardless of finding severity*, unless otherwise authorized by CMS. If additional time is required, *follow* the *process specified within section 3.5.2.*

    - *The 90-day finding resolution requirement does not include findings identified by the Cyber Risk Management (CRM) program at CMS (e.g., Known Exploitable Vulnerabilities (KEVs), Common Vulnerabilities and Exposures (CVEs), etc.). These types of findings relate to patch management and shall follow the requirements set forth in the BPSSM, Section 3.10 - Patch Management.*

- The contractor shall document system security controls in the CMS FISMA Controls Tracking System (CFACTS) tool to demonstrate compliance with MAC ARS controls and documentation. The contractor shall also use CFACTS to maintain documentation that supports the Authority to Operate (ATO) process, including certification of the documentation.

- 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 appoint a Chief Information Officer (CIO) to oversee its compliance with the CMS information security requirements. The contractor's principal Systems Security Officer (SSO) shall be a full-time position dedicated to assisting the business partner CIO in fulfilling these requirements.

- The contractor must implement systems in a manner that is compliant with the CMS Target Lifecycle (TLC) and the Technical Reference Architecture (TRA). When directed by CMS, compliance with the TLC and the TRA will be demonstrated by presenting system updates to the CMS Technical Review Board (TRB). For situations where the TRA conflicts with the MAC ARS, the MAC ARS shall take precedence.

- The contractor shall meet all contingency planning and disaster recovery requirements included in the MAC ARS and the Business Partners Systems Security Manual (BPSSM), with the goal of restoring key claims processing and operations within 72 hours.

- The contractor shall review, update and approve all policies and procedures every 365 days and not every three years as stated in the MAC ARS.

- *The contractor shall review system accounts (as defined in ARS control AC-02), at least once every ninety (90) days. Any other accounts shall be reviewed at least annually.*

2 – Information Technology (IT) Systems Security Roles and Responsibilities

2.1 - Key Personnel Roles

(Rev. 15.1; Issued: 07-17-25; Effective: 02-28-25; Implementation: 08-18-25)

Key Requirements
Business partners shall designate a principal (i.e., primary) SSO who is qualified to manage the Medicare information security 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.

See Section 1.1 for additional requirements that pertain to the Medicare Administrative Contractor SSO position.

The business partners that process Medicare data shall maintain an Authority to Operate (ATO) for the information technology systems that are used. The ATO requires that certain roles be filled by Federal personnel and other roles to be filled by business partner personnel. Many of the roles, and the associated responsibilities, are listed in the CMS Information Systems Security and Privacy Policy (IS2P2) and the HHS Information Systems Security and Privacy Policy (IS2P)[1] manuals. Some of the key personnel listed in the IS2P2 include:

- Business Owner (BO)
- Contracting Officer Representative (COR)
- Information System Security Officer (ISSO)
- System Developer Maintainer (SDM)

In addition to the above roles, the business partner personnel shall include a principal System Security Officer (SSO). The 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. The SSO should also encourage their systems security personnel to pursue security accreditation.

A business partner may have additional SSOs at various organizational levels, but all security actions that affect Medicare operations shall be coordinated through the principal SSO. The *principle* SSO ensures compliance with the CMS information security program and MAC ARS by:

- Facilitating the Medicare IT system information security program and ensuring that necessary safeguards are in place and working
- Coordinating information security system activities throughout the organization
- Ensuring that IT system information security requirements are considered during budget development and execution
- Reviewing compliance of all components with the MAC ARS and reporting vulnerabilities to management
- Ensuring an incident response capability is established for investigating system security and privacy breaches and reporting significant problems (see section 3.6) to business partner management and CMS

[1] The HHS IS2P document is available by requesting it from your Federal Information System Security Officer

- Ensuring that technical and operational information security controls are incorporated into new IT systems by participating in and reviewing all new systems/installations and major changes

- Ensuring that IT systems information security requirements are addressed in Requests for Proposal (RFP) and subcontracts involving the handling, processing, and/or analysis of Medicare data

- Maintaining information security documentation in the System Security Profile for review by CMS and external auditors and keeping all elements of the System Security Profile (see section 3.7)

- Cooperating in all official external evaluations of the business partner's information security program

- Facilitating the completion of the Information Security Risk Assessment (see section 3.2)

- Ensuring that an operational IT Systems Contingency Plan (ITSCP) is in place and tested (see section 3.3)

- Documenting and updating the monthly Plan of Action and Milestones (POA&M) (see section 3.5.2). *Additional updates* may occur whenever a POA&M scheduled completion date passes, and/or following the issuance of new requirements, risk assessments, internal audits, and external evaluations

- 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 shall earn a minimum of 40 hours in continuing professional education credits each year. The educational sessions conducted at the CMS Security Controls Oversight and Update Training (CSCOUT) can be u
sed toward fulfilling the continuing professional education credits. The associated credit hours will be noted on the CSCOUT agenda.

2.2 – Personnel Security/Suitability

(Rev. 15)

All business partner and contractor personnel requiring access to CMS sensitive information shall meet minimum personnel suitability standards. These suitability standards are based on a valid need-to-know (not based on position or title) and favorable results from a background check. Each position must be evaluated and assigned a risk and/or a sensitivity designation commensurate with each individual's duties and responsibilities. The background check for prospective employees shall include, at a minimum: Social Security Number verification, identity and address verification, national criminal database search, county criminal records search, HHS list of excluded individuals, sex offender registry, verification of academic records when required for the position and verification that the employee has resided in the US for 3 of the past 5 years.

When required by CMS, business partner personnel will need to complete a Federal Background Investigation (BI). To initiate a BI, business partner personnel will need to supply personal information to CMS via methods (fingerprint card) or systems identified by CMS. The level of

investigation for a BI varies and will be determined by the COR's risk assessment of the person's role. A BI that results in a favorable outcome can result in a Personal Identity Verification (PIV) card being issued.

3 - IT Systems Security Program Management

(Rev. 15.1; Issued: 07-17-25; Effective: 02-28-25; Implementation: 08-18-25)

Key Requirements
The Security Program consists of several fundamental components that are all designed to implement controls and to reduce risk. Key elements of controls include Policies, Procedures, Technical Implementations, Standards, and Management Reviews.

Required security documentation includes, but is not limited to, the system security *and privacy* plan, the information security risk assessment, and the IT systems contingency plan.

Business partners shall implement an IT Systems Security Program to manage system security risks. Risks are identified by the business partner in the Information Security Risk Assessment (see section 3.2) and the security requirements are documented in the System Security *and Privacy* Plan (see section 3.1). The underlying support for these documents is the controls implemented by the business partner. Information system security controls shall be implemented in a consistent manner everywhere within the system's accreditation boundary to protect the CIA of sensitive information. In addition, testing shall be performed to ensure that information security controls are operating as intended.

3.01 – Control Components

(Rev. 15.1; Issued: 07-17-25; Effective: 02-28-25; Implementation: 08-18-25)

Business partners shall have policies and procedures and implement controls or plans that fulfill the MAC ARS controls. The business partner Medicare claims related security program shall be based on the MAC ARS (IOM 100-17, Attachment 1), the BPSSM (IOM 100-17) and on the collection of CMS policies, procedures, standards, and guidelines found on the CMS Information Security Web site at: *https://security.cms.gov*

Policies are formal, up to date, documented rules that are tailored to the environment, are communicated as "shall" or "will" statements and are readily available to employees. They establish a continuing cycle of assessing risk, implementing controls and 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.

Technical Implementations are the acquisition and installation of hardware, software, or assets to be used for the establishment of a new control, or the improvement of an existing control. The intention of a technical implementation is to automate or facilitate a control process that would otherwise be manually performed.

Standards are formal, written, mandatory actions, rules, or specifications designed to support and conform to a policy or procedure. A standard must include one or more accepted specifications for configurable items for hardware, software, or behavior. Standards are often required to successfully complete technical implementations and can be either part of policies and procedures or can be standalone documents. Standards can result from, either exclusively by or in combination with, laws promulgated by governing bodies, obtained from known standards organization or developed by the business partner using industry best practices.

Management Review is the business partners' formal oversight activity of control implementations and should be performed at various management levels. Oversight is a regular activity to verify that the control environment for which management has responsibility is functioning properly. Management must set benchmarks or other methods to measure the success of controls. Where appropriate, management should document their review by formally approving evidence supplied.

3.02 – Reporting Requirements

(Rev. 15.1; Issued: 07-17-25; Effective: 02-28-25; Implementation: 08-18-25)

Key Requirements
Business partners are required to provide documentation to CMS regarding the status of their IT security program. Documentation shall be reported to CMS according to the appropriate procedures, which are summarized in Table 3.1.

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.

In addition, Table 3.1 indicates how often these requirements 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)
System Security Profile – Section 3.7	As necessary	• On file with the Principal SSO	The System Security Profile documents may be stored as paper documents, electronic documents, or any combination thereof.	
CMS Annual FISMA Assessment (FA) – Section 3.5.1	One third of the controls shall be tested each year so all controls are tested during a 3-year period.	• COR with a copy to CMS CO via CFACTS • System Security Profile	FA results recorded in the CFACTS are to be discussed in the Certification Package for Internal Controls (CPIC).	
System Security *and Privacy* Plan (*SSPP*) – Section 3.1	The *SSPP* for each General Support System (GSS) and MA shall be reviewed, updated, and approved by management every 365 days, or upon significant change[2].	• CMS CO via CFACTS • System Security Profile	Information system security *and privacy* plans are to be generated via CFACTS, reviewed, updated, and approved by management and the approved *SSPP* saved in CFACTS, the CPIC and Statement of Certification, and the System Security Profile.	
Information Security Risk Assessment – Section 3.2	The information security risk assessment for each GSS and MA shall be reviewed, updated, and approved by management every 365 days, or upon significant change.[1]	• CMS CO via CFACTS • System Security Profile	Information security risk assessments are to be *generated via CFACTS,* reviewed, updated, and approved by management and saved in the CFACTS, the CPIC and Statement of Certification, and the System Security Profile. The information security risk assessment is submitted with the system security *and privacy* plan[3].	
Certification (CPIC) – Section 3.4	Each federal FY	• COR with a copy to CMS CO via CFACTS • System Security Profile	Business Partners should include a statement of certification as part of their CPIC. Each year CMS will publish in Chapter 7 (Internal Controls) of its Financial Management Manual (Pub 100-06) 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 CORs.	
IT System Contingency Planning – Section 3.3	CPs shall be reviewed, updated, and approved by management every 365 days, or upon significant change.[1] CPs shall be tested annually.	• CMS CO via CFACTS • System Security Profile	Business partner management and the Business Owner shall approve the CP. The ITSCP is to be developed (in accordance with Appendix A and CMS RMH documents), reviewed, updated, and approved by management—and saved in CFACTS, the Certification Package/Statement of Certification, and the System Security Profile[4].	

[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 Risk Assessment Reports can be found in the CMS risk assessment procedures.

[4] More information about contingency planning can be found in *the latest version* of the NIST SP 800-12, An Introduction to Computer Security: The NIST Handbook, and NIST SP 800-34, Contingency Planning Guide for Federal Information Systems.

Requirement	Frequency	Send To	Comments	Complete (check when complete)
Plan of Action and Milestones – Section 3.5.2	Each federal FY	• ISSO • COR • CMS CO via CFACTS • System Security Profile	POA&Ms address findings of internal/external audits/reviews including annual security assessments, and, as applicable: Statements on Standards for Attestation Engagements (SSAE) 18 reviews, A-123, Chief Financial Officer (CFO) controls audits, the Section 912 evaluation, *delayed weaknesses (configuration management, vulnerability management)* and data center tests and reviews.	
Incident Reporting and Response – Section 3.6	As necessary	• COR • CMS IT Service desk • Medicare Contractor Management Group (MCMG) Security Mailbox (See the latest guidance from CMS for more information) • System Security Profile	Health Insurance Portability and Accountability Act (HIPAA), Health Information Technology for Economic and Clinical Health Act (HITECH) and the Privacy Act of 1974 addresses Incident Reporting information.	
Authorization To Operate – Section 3.8	As necessary to acquire and maintain a CMS CIO-granted Authorization to Operate.	On file with CMS Information Security and Privacy Group (ISPG), with a copy maintained in the CFACTS.		

TABLE 3.1 LEGEND:

CFACTS	CMS FISMA Controls Tracking System
CFO	Chief Financial Officer
CO	Central Office (CMS)
COR	Contract Officer Representative
ITSCP	IT System 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
IT	Information Technology
MA	Major Application
POA&M	Plan of Action and Milestones
RA	Risk Assessment
SSAE	Statement on Standards for Attestation Engagements
SP	Special Publication (NIST)
SSO	Business Partner Systems Security Officer

When documentation *cannot be submitted electronically*, Registered Mail™ or its equivalent (signed receipt required) shall be used. Contact the appropriate COR or ISSO for the correct address.

3.1 - System Security *and Privacy* Plan (*SSPP*)

(Rev. 15.1; Issued: 07-17-25; Effective: 02-28-25; Implementation: 08-18-25)

Key Requirements
Business partners are required to update and re-certify the *SSPP* every 365 days unless there are changes that would necessitate a more frequent update. Updates to the *SSPP* shall be performed via CFACTS.

Defining a system boundary is a key step that must be completed before *an SSPP* can be accurately documented.

The *SSPP* should address how the control environment is implemented to mitigate risks identified in the information security risk assessment.

The objective of an information security program is to *maintain and* 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 SSPP*. The completion of *an SSPP* is a requirement of the Federal Information Security Management Act of 2014 (FISMA), Privacy Act of 1974, As Amended, Office of Management and Budget (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 *SSPPs*.

The purpose of *an SSPP* is to provide an overview of the security *and privacy* requirements of a system and describe the controls that are implemented to meet those requirements. The *SSPP* also delineates responsibilities and expected behavior of all individuals who access the system. The *SSPP* 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 security *and privacy* plans for their Medicare claims-related GSSs and MAs in both the CFACTS and their System Security Profiles. The *SSPP* documents the current level of security within the system or application; that is, actual implemented controls, not planned controls. In addition, the *SSPP* serves as the primary documentation reference for testing and evaluation, whether by CMS, the General Accounting Office (GAO), or other oversight bodies. The *SSPP* is a sensitive document, as it may discuss uncorrected vulnerabilities and may mention risks that have been accepted. Therefore, security *and privacy* plans should be distributed only on a need-to-know basis.

The *SSPP* shall be recertified by business partner management and the signed copy made available to the SSO and authorized external auditors as required. The SSO and business partner are responsible for reviewing the *SSPP* 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 *SSPPs* shall be developed and documented in accordance with the latest instruction from CMS.

SSPP shall be recertified within 365 days from the previous certification date. The *SSPP* shall also be reviewed prior to recertification (within the original certification timeframe) to determine whether an update is required. The *SSPP* 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 *SSPP*, if applicable, shall be documented in the CFACTS, and placed in the System Security Profile.

Contractors updating their current security *and privacy* plan(s) or developing new security *and privacy* plan(s) shall take into account Medicare claims processing front-end, back-end, and/or other claims processing related systems.

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.

Within 10 business days of updating, developing or recertifying an *SSPP*, CFACTS must be updated.

3.2 – Information Security Risk Assessment (ISRA)

(Rev. 15.1; Issued: 07-17-25; Effective: 02-28-25; Implementation: 08-18-25)

Key Requirements
Business partners are required to perform an annual ISRA in accordance with the most current versions of the CMS ISRA procedures available on the CMS Web site at: *https://security.cms.gov.* The identified risks will aid in the design of controls to satisfy the MAC ARS.

Documentation of the risks needs to be completed before a control is designed and implemented. Controls should be designed to be cost effective based on the risk to the operating environment.

Risks never go away but can increase as new vulnerabilities are found and decrease as new or enhanced controls are implemented.

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 risk assessment procedures shall be used to prepare an annual ISRA.

ISRAs shall be *updated and* recertified within 365 days from the previous certification date. The ISRA shall also be reviewed prior to recertification (within the original certification timeframe) to determine whether an update is required. The ISRA 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 ISRA, if applicable, shall be *maintained* in the System Security Profile and *CFACTS.* Note that the ISRA used to support *an SSPP* cannot be dated more than 365 days earlier than the security *and privacy* plan certification date.

Within 10 business days of updating, developing or recertifying an ISRA, CFACTS must be updated.

3.3 – IT Systems Contingency Plan (ITSCP)

(Rev. 15.1; Issued: 07-17-25; Effective: 02-28-25; Implementation: 08-18-25)

Key Requirements
Business partners are required to document and test an ITSCP in accordance with the most current versions of the CMS Information Security Contingency Planning standards and procedures available within Appendix A of this document and on the CMS web site at: *https://security.cms.gov.*

All business partners are required to develop and document an ITSCP 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. The ITSCP shall be included in management planning and shall be:

- Reviewed as part of a documented System Development Life Cycle, whenever new systems are planned or upon significant change
- Reviewed when new safeguards are implemented
- Reviewed and approved within 365 days to ensure accuracy
- Tested within 365 days. 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, DME]), each individual Medicare contract type shall be tested every 365 days.

Approved plans*,* test reports (results) *and appropriate dates* shall be maintained in *the* CFACTS and placed in the contractor's System Security Profile. Business partner management*, the SSO,* and the *CMS Business Owner* shall approve newly developed and/or updated ITSCPs. A newly *approved* IT Systems CP shall be updated in the CFACTS and submitted to CMS within 10 business days.

Appendix A to this manual provides information on ITSCP and testing methods. Also, see Table 3.1 for additional information.

3.4 – Certification Package for Internal Controls (CPIC)

(Rev. 15.1; Issued: 07-17-25; Effective: 02-28-25; Implementation: 08-18-25)

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 MAC ARS controls. 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 information security compliance within each federal Fiscal Year (FY). This security certification shall be included in the CPIC or, for contracts not required to submit CPICs, send the security certification to their appropriate CMS CORs. 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.

System 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 *and Privacy* Plan for each GSS and MA (see section 3.1)
- Information Security Risk Assessment (see section 3.2)
- IT Systems Contingency Plan (see section 3.3 and Appendix A)
- Plan of Action and Milestones (see section 3.5.2)

3.5 - Compliance

(Rev. 15)

Compliance refers to the contractual obligations of business partners to CMS. The components to comply with IT security requirements are described in detail in the following subsections.

3.5.1 - Annual FISMA Assessment (FA)

(Rev. 15.1; Issued: 07-17-25; Effective: 02-28-25; Implementation: 08-18-25)

Key Requirements
At least 1/3 of controls must be tested each year, and all controls shall be tested over a 3-year period. CMS identifies which control families must be tested each year.

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 MAC ARS controls 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 MAC ARS controls shall be tested. This means a subset (no less than one-third [$^1/_3$]) of the MAC ARS controls shall be tested each year so that all security controls are tested during a 3-year period. In an effort to standardize testing and results summarization, a 3-year rotation of MAC ARS control families was established by CMS. After the 3-year rotation is completed, the testing rotation shall be repeated until notification from CMS is received. As control families are added or removed, CMS reserves the right to change the controls that must be tested each year.

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 organization's 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 MAC ARS effectiveness. All management-directed and independent testing conducted within 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. 15.1; Issued: 07-17-25; Effective: 02-28-25; Implementation: 08-18-25)

Key Requirements
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&Ms in the CFACTS and, if required by CMS, uploading any additional supporting documentation.

All security and privacy related findings shall be entered into CFACTS. *Security and privacy findings include* findings from Section 912, FISMA, CFO, security control assessments, penetration tests, Statement on Standards for Attestation Engagement No. 18 (SSAE-18) and all other reviews and audits.

3.5.2.1 - Background

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 are also 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 recorded in CFACTS.

Section 912 of the MMA implemented requirements for annual evaluation, testing, and reporting on security programs for MAC 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 and CMS. 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.

CFACTS enables contractors to satisfy reporting requirements for security and privacy related findings. Security and privacy related findings and approved action plan data is promptly entered into the CFACTS following all audits/reviews.

3.5.2.2 - POA&M Components/Submission Format

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

The CFACTS shall be populated and maintained with security and privacy 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 reporting requirements. In addition to the initial POA&M reporting that follows each audit/review, ongoing milestones for all corrective action plans will be updated on the 1st business day of each month.

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

Monthly Reporting. 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. *Milestones that have a status of Completed or Not Started do not need to be updated monthly.*

***Delayed Resolution**. If the contractor needs additional time to complete a POA&M beyond 90 days, then the following process should be followed:*

- *A milestone describing the mitigating/compensating controls in place shall be documented in CFACTS.*
- *For audits or evaluations that are initiated by CMS, the contractor shall email the DMSSOO and the appropriate COR(s) to request approval to extend the completion date. Included with the request, the contractor shall document the circumstances surrounding the extension and the new estimated completion date. The DMSSOO will respond documenting whether the extension is granted.*
- *For all other internal audits or evaluations conducted by the contractor, the contractor shall notify DMSSOO and the appropriate COR(s) via email the need and reason to extend*

the scheduled completion date along with the new scheduled completion date. The DMSSOO will respond documenting the acknowledgement.

3.5.3 - Timing Requirements for Compliance Conditions

(Rev. 15.1; Issued: 07-17-25; Effective: 02-28-25; Implementation: 08-18-25)

Key Requirements

In the MAC ARS, many security documents and recurring processes (e.g., log reviews, access reviews, document reviews, etc.) require timely execution on a yearly, bi-annual (every 6 months), quarterly, monthly, weekly or daily basis.

It is important to note that events such as Penetration Tests, Contingency Plan Tests, Federal Information Security Management Act (FISMA) Submissions, etc. are not subject to the timing conditions described below.

In order to assure that *security* documents *and recurring* processes*, as defined above,* are reviewed/processed timely, the following timing requirements apply:

- Yearly/365 days: Any document/process to be reviewed on a yearly basis shall be performed *no later than* the same *calendar* month each year. For example, if you review your ISRA or ITSCP on February 14th, then the next review must take place *no later than* the *end* of February during subsequent years. This can be applied to reviews to be performed over multiple years. If you perform a review in February and a review is due 3 years later, it must be *performed no later than* the *end* of February for the year when the review is to be performed again. 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 an annual review is performed prior to the month of the last annual review, this month now needs to be considered the calendar month for the annual review the following year.*

- Bi-Annual/Every 6 Months/180 days: The months designated for a 6-month document/process review shall occur every 6 months and be consistent from year to year. For example, if you perform an initial review during February, then the next review must be performed within the month of August. In subsequent years, the review must be performed within the months of February and August. Those months then become your standard months for performing the review.

- Quarterly/90 days: The months designated for a quarterly document/process review shall occur every 3 months and be consistent from year to year. A quarterly document/process review shall be scheduled on the same day of each designated month and be performed within 4 business days** before or after the scheduled review date of those months. That is, if you choose July 16 as your review date, then your review date will be the 16 in each designated month. The following table demonstrates when quarterly reviews must be performed based on the day your scheduled review date occurs.

Earliest Review		Review Target Day	Latest Review
Previous Tuesday		Monday	Following Friday
Previous Wednesday		Tuesday	Following Monday
Previous Thursday		Wednesday	Following Tuesday
Previous Friday		Thursday	Following Wednesday

Previous Monday		Friday	Following Thursday

**Federal holidays or incidental office closures will not affect these timeframes.

- Monthly/30 days: The document/process review shall be performed within 2 business days** before or after the scheduled review *completion* date each month. The exact date of the monthly review shall not change month to month. That is, if you choose July 16th as your review *completion* date, then your review date will be the 16th in every subsequent month. The following table demonstrates when monthly reviews must be *completed* based on the day your scheduled review date occurs.

Earliest Review	*Completed* Review Target Day	Latest *Completed* Review
Previous Thursday	Monday	Following Wednesday
Previous Friday	Tuesday	Following Thursday
Previous Monday	Wednesday	Following Friday
Previous Tuesday	Thursday	Following Monday
Previous Wednesday	Friday	Following Tuesday

**Federal holidays or incidental office closures will not affect these timeframes.

- Weekly/7 days: Weekly/7 days document/process reviews shall be performed on the same day every week. If the scheduled review day falls on a holiday, the previous or subsequent business day can be used as your review target date, returning to the original target date in subsequent weeks.

- Daily/24 hours: Daily/24 hours document/process reviews shall be performed on the next business day. If the day of the scheduled review falls on a Saturday, then the review is performed on a Monday. If the day of the scheduled review falls on a federal holiday or an incidental office closure, then the review is performed the next business day. This may cause more than one review to be performed on the same day.

If the business partner wishes to change the timing cycle of a review, the business partner is required to shorten the timing cycle and not lengthen the timing cycle to attain the new performance date. For example, if the annual/yearly review of the security *and privacy* plan is being performed in June during year 1 and the business partner desired to change the review date for year 2, they would be required to review the security *and privacy* plan in a month prior to June. That month would then become the review month going forward.

Exceptions to the timing requirements can be implemented with the approval of the CMS ISSO. These can be one-time exceptions (e.g., a yearly review of a disaster recovery test is performed after an established month due to scheduling issues with the recovery facility).

3.6 - Security Incident Reporting and Response

(Rev. 15.1; Issued: 07-17-25; Effective: 02-28-25; Implementation: 08-18-25)

Key Requirements
All security incidents shall be reported to CMS in accordance with the requirements listed in the CMS Risk Management Handbook (RMH) Chapter 8. Incidents shall be reported to the IT Service Desk. A security incident is *a Personally Identifiable Information (*PII*)* or *Protected Health Information (*PHI*)* breach, a ransomware event, or an event that impacts the confidentiality, integrity or availability of Medicare data.

Final reports for all incidents shall be submitted timely but no later than 40 days after the initial reporting of an incident.

MACs shall also email each incident report to mailto:Security_Incident@cms.hhs.gov.

NIST Special Publication 800-*61* defines a computer*/cybersecurity incident as an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or constitutes* a violation or imminent threat of violation of *law,* security policies, *security procedures, or* acceptable use policies. Examples of incidents are:

- An attacker commands a botnet to send high volumes of connection requests to a web server, causing it to crash.
- Users are tricked into opening a "quarterly report" sent via email that is actually malware; running the tool has infected their computers and established connections with an external host.
- An attacker obtains sensitive data and threatens that the details will be released publicly if the organization does not pay a designated sum of money.
- A user provides or exposes sensitive information to others through peer-to-peer file sharing services.

An "imminent threat of violation" refers to a situation in which the organization has a factual basis for believing that a specific incident is about to occur. For example, the antivirus software maintainers may receive a bulletin from the software vendor, warning them of new malware that is rapidly spreading across the Internet.

The business partner shall use its security policy and procedures to determine whether a non-reportable event or a reportable security incident has occurred. Examples of non-reportable events include a user connecting to a file share, a server receiving a request for a web page, a user sending email or a firewall blocking a connection attempt. Upon receiving notification of an IT systems security incident or a suspected incident, the SSO or another identified individual shall immediately perform an analysis to determine if an incident actually occurred. The incident should be evaluated to determine if it impacts the processing of Medicare data or the confidentiality, integrity and availability of Medicare data.

All suspected security incidents or events shall be reported to the business partner's IT service desk (or equivalent business partner function) as soon as an incident comes to the attention of an information system user. All security incidents and events shall be reported to the CMS IT Service Desk in accordance with the procedures set forth in the CMS RMH Chapter 8 Incident Response. This document is available on the CMS Information Security Web site at https://security.cms.gov/. The CMS IT Service Desk can be contacted by telephone at 800-562-1963 or 410-786-2580, or by e-mail at: mailto:CMS_IT_Service_Desk@cms.hhs.gov. Contacting the CMS IT Service Desk by telephone is *highly* recommended if immediate action by CMS is required. In addition, MACs shall also email each incident report to mailto:Security_Incident@cms.hhs.gov.

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 affected 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 Office of Inspector General

(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 CISO.

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 ISRA. Business partners shall refer to CMS RMH Chapter 8 Incident Response manual for further guidance.

Many of the PII breaches being reported to CMS occur when unencrypted emails are sent to the intended recipients. A mitigating control to allow many of these breaches to be closed more easily is the implementation of the Transport Layer Security (TLS) protocol within email servers such as Microsoft Exchange. The TLS protocol encrypts emails for transmission between two email servers. There are different TLS features which can be used and provide different levels of assurance that an email will be encrypted. Use of any of these features requires TLS to be enabled. To mitigate the severity of email PII breaches, business partners are required to enable TLS on their email servers. In addition, the most secure TLS feature that can be enabled to encrypt emails between business partners shall be implemented. If a business partner cannot implement TLS, a risk must be documented in the *ISRA*.

3.7 - System Security Profile

(Rev. 15.1; Issued: 07-17-25; Effective: 02-28-25; Implementation: 08-18-25)

Key Requirements
The System Security Profile is a copy of the documents that are maintained in *the* CFACTS and *submitted to* CMS *as requested*. These documents shall be available if business partner management requires timely access to them without *the* CFACTS.

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

- Completed FAs
- *SSPP*
- *ISRA*
- Certifications
- *ITSCP*
- POA&Ms for each compliance security review
- POA&Ms for other security review undertaken by Department of Health and Human Services (*DHHS*) OIG, CMS, Internal Revenue Service (IRS), GAO, consultants, subcontractors, and business partner security staff
- Incident reporting and responses
- Systems information security policies and procedures

3.8 - Authorization To Operate

(Rev. 15.1; Issued: 07-17-25; Effective: 02-28-25; Implementation: 08-18-25)

Business partners are required to acquire and maintain a CMS issued Authorization to Operate (ATO) for each FISMA system. To maintain an ATO, the business partner is expected to maintain all security documentation in CFACTS, and the documentation must be up to date as defined in BPSSM table 3.1. When applying for an ATO, critical and high risk POA&Ms must be in either a pending verification status or mitigated so the risk can be demonstrated to be moderate or low.

3.9 – Identity Proofing

(Rev. 15.1; Issued: 07-17-25; Effective: 02-28-25; Implementation: 08-18-25)

Key Requirements

Identity proofing establishes that a user (both organization and non-organizational) is who the user claims to be. Identity proofing is the process of collecting, validating, and verifying user's identity information for the purposes of issuing credentials for accessing a system.

Assuring appropriate identity evidence, such as documentary evidence or a combination of documents and biometrics, reduces the likelihood of individuals using fraudulent identification to establish an identity, or at least increases the work factor of potential adversaries.

Care should be taken to ensure that only the absolute necessary information be obtained in order to keep the amount of PII that is collected to a minimum.

Business partners shall assure that users are effectively identity proofed in accordance with ARS control requirements. To assure that users are properly identified and validated, it is imperative that business partners apply consistent identity proofing concepts.

To properly identity proof users, business partners shall implement a process that meets the requirements identified within NIST 800-63A and meets or exceeds standards for IAL2.

It is not a requirement that identity proofing be done in person.

Exceptions and situations that require further clarification should be discussed with CMS before *implementation.*

3.10 - Patch Management

(Rev. 15.1; Issued: 07-17-25; Effective: 02-28-25; Implementation: 08-18-25)

Key Requirements
The timely patching of systems is one of the critical controls to preventing network intrusions.

The MAC ARS requires the correction of identified security-related information system flaws on production equipment based on a frequency / time frame documented in the applicable system's patch management plan. The time frame begins when the vendor releases a patch, not when the business partner becomes aware of a patch. The patching requirement is 15 calendar days for all critical patches and 30 calendar days for all other patches. *If a flaw cannot be effectively addressed within that timeframe, documentation shall be maintained to track and remediate it. If a vulnerability is identified but a patch is not yet available, documentation shall be maintained to track and remediate the vulnerability if the timeframe exceeds the patching requirement outlined above.*

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

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 *in accordance with the requirements documented* in Table 3.3 below for 1) Patch Identification, 2) Patch Installation and 3) Unsupported software.

Table 3.3

Patch Identification	Include all patches that are released from the system, application, or device vendor. All patches must be analyzed by the business partner to determine their applicability and security impact on the operating environment. All patches analyzed from the vendor must be tracked through a formal process and categorized as 1) Security or 2) Operational in nature.
Patch Installation	All security patches risk ranked as critical shall be implemented in 15 calendar days. All other security patches, regardless of the patch risk ranking, shall be implemented in 30 calendar days. Security related patches not installed based on business partner analysis shall be documented with an appropriate business justification that includes security impact, operational impact, business impact, mitigating or compensating controls, and residual risk. Re-evaluation of the justification must be performed within every 365 days.
Unsupported Software	Unsupported software, or software that is not formally supported by the software vendor for security or

	operational patches, shall not be used unless advanced patch support is purchased or provided through another documented source. All unsupported software in operation shall be documented within the Business Partner's ISRA and POA&M with phase out timelines defined. For details, see section 3.12 – End of Life Technology Components.

The current version of NIST SP 800-40 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.

3.11 - Security Configuration Management

(Rev. 15.1; Issued: 07-17-25; Effective: 02-28-25; Implementation: 08-18-25)

Key Requirements

Business partners are required to create a security baseline for the configuration of the information system components. A baseline is a formal, management approved standard that documents the customization of Federal or other guidelines.

The process for establishing and maintaining baselines shall allow misconfigurations to be identified and risk-minimized, including a documented process that supports timely resolution of misconfigurations.

Federal guidelines should be used to create baselines. If a Federal guideline does not exist, hardening guides or documented best practices may be used.

DMEMACs *and* ABMACs are responsible for starting their security configurations with the Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) Checklists when creating a baseline. All appropriate or referenced DISA checklists and guidelines shall be considered for input into each baseline.

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

Misconfigurations are defined as:

- A setting that violates a configuration policy or that permits or causes unintended behavior that impacts the security posture of a system.
- An incorrect or suboptimal configuration of an information system or system component that may lead to vulnerabilities.

In order to effectively protect MAC environments from vulnerabilities produced by incorrectly configured information system components, any misconfiguration shall be updated/corrected within 30 days from the time of discovery. If the misconfiguration cannot be effectively addressed within that timeframe, a POA&M shall be opened to track and remediate misconfigured setting(s).

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 Federal security configuration guidelines follows. If there is a conflict between the MAC ARS and a DISA STIG, the MAC ARS takes precedence. See Table 3.4 for more information. If there are any other questions or concerns about resolving conflicts among security configuration guidelines, business partner SSOs shall contact their CMS ISSO.

Table 3.4

Business Partners	DMEMAC/ABMAC
1. MAC ARS 2. United States Government Configuration Baseline (USGCB) 3. NIST National Checklist Program (NCP) / NIST 4. DISA	1. MAC ARS 2. DISA/USGCB 3. NIST National Checklist Program (NCP) / NIST / Center for Internet Security (CIS) / *Cybersecurity and Infrastructure Security Agency (CISA) / Other Federal Guidance* 4. Vendor supplied guidance

3.11.1 - Security Technical Implementation Guides (STIG)

(Rev. 15.1; Issued: 07-17-25; Effective: 02-28-25; Implementation: 08-18-25)

Security guidelines, called STIGs, 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. STIGs are developed by DISA to help system operators configure security within their systems to the highest level possible. DISA also has made available Security Requirement Guides (SRGs) for certain platforms. These guidance documents may be intended to use along with STIGs as the security guidelines for a specific platform. All STIGs and SRGs are available from DISA. The link for these documents is https://public.cyber.mil/stigs/compilations/. CMS recommends that business partner SSOs (or their designated representative) subscribe to the DISA STIG-News Mailing List at: https://public.govdelivery.com/accounts/USDISA/subscriber/new?topic_id=USDISA_181 so they will be notified whenever updated or new STIG Checklists become available.

The use of latest publicly available DISA STIG is mandatory for all business partner systems/applications that process, store, and/or transmit Medicare claims data. DMEMACs *and* ABMACs are required to start with the STIG configurations and then document a customized baseline with any deviations based on environment specific implementation. In the event that DISA does not have a STIG available for a specific platform, business partners should follow the defined CMS hierarchy within the MAC ARS controls.

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 viable, and to implement all settings that are found to be feasible. Settings that cannot be implemented across an entire platform (e.g. Windows 2019, AIX) shall be documented as "system deviations." Customized baseline values (including those that may already be "system deviations") that cannot be implemented on only specific systems shall be documented as "system exceptions,". All STIG

recommended security settings that are determined not to be viable in a business partner environment (including “system exceptions”) 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.

3.11.2 - United States Government Configuration Baseline (USGCB) Standard

(Rev. 15.1; Issued: 07-17-25; Effective: 02-28-25; Implementation: 08-18-25)

The purpose of the United States Government Configuration Baseline (USGCB) initiative is to create security configuration baselines for Information Technology products widely deployed across federal agencies. The USGCB baseline evolved from the Federal Desktop Core Configuration (FDCC) mandate. While not addressed specifically as the FDCC, the process (now coined the USGCB process) for creating, vetting, and providing baseline configurations settings was originally described in a 22 March 2007 memorandum from OMB to all Federal agencies and department heads and a corresponding memorandum from OMB to all Federal agency and department Chief Information Officers (CIO).

Business Partners have the choice of using the USGCB configurations or the STIGs for the platforms listed on the USGCB Web site at https://csrc.nist.gov/projects/united-states-government-configuration-baseline.

3.11.3 - National Institute of Standards and Technology (NIST)

(Rev. 15)

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 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.

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 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 Business Partners Systems Security Manual (BPSSM) and the MAC ARS. 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.

3.12 - End of Life Technology Components

(Rev. 15.1; Issued: 07-17-25; Effective: 02-28-25; Implementation: 08-18-25)

The current HHS policy states "Operating systems, software and applications are considered end-of-life (EOL) when they are no longer supported by the vendor/provider and do not receive product updates and security patches." Standard HHS contract language requires that vendor software needs "to be within one major version of the current version". To address both the HHS policy and the HHS contract language, and to document how the business partner has implemented the EOL control, business partners need to implement MAC ARS control SA-22, which restricts the use of unsupported information system components. For business partners, components are defined as any hardware or software used by the FISMA system.

While paying for extended support to receive security updates for all levels of severity (with a component vendor or a third-party vendor) is acceptable for meeting the HHS policy regarding EOL, business partners are expected to plan for and remove components that the vendor plans to, or currently no longer supplies security updates. If vendors can only provide updates or fixes for certain levels of security flaws (e.g. critical only), this could leave security threats and risks present in the environment and would not be acceptable for meeting the HHS policy regarding EOL.

Business partners shall demonstrate their efforts to remove these components, with documentation that can include, but is not limited to, vendor notifications, project plans and identified issues. If the components cannot be removed before security updates end because the vendor provided limited notice or because removal requires a long-term project, then the business partner shall work with CMS to implement controls to mitigate risk to an acceptable level until the component can be replaced. If the risk cannot be sufficiently reduced, the business partner shall work with CMS to open a POA&M, if necessary, prior to the end of support. In addition, business partners are required to be on either the current or the one prior major version of the component. For those situations where the business partner wants to use previous versions, and the component is supported by the vendor, then the business partner shall perform a risk analysis and document the results in the ISRA.

3.13 - Cloud Computing

(Rev. 15.1; Issued: 07-17-25; Effective: 02-28-25; Implementation: 08-18-25)

According to NIST, cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. (NIST SP 800-45). FEDRAMP has implemented security requirements for low, moderate and high risk rank systems. MACs and other business partners that are rated as high can use CSPs with the approval *of the CMS COR and concurrence* of

the CMS ISSO. MACs are expected to document control implementations and confirm compliance of CSP controls within their *SSPP*. If the CSP supplied controls and services are less strict than the MAC ARS requirements, then the business partner is expected to supplement the CSP controls or implement separate controls that meet the MAC ARS. Also, other requirements that are not specifically documented in the MAC ARS or in an RMH document, such as the reporting of configuration settings are not waived with the use of a CSP; therefore, this should be carefully considered before requesting to use a CSP.

When utilizing a CSP, MACs must perform the following actions:

1. *Maintain a responsibility line matrix that defines MAC control responsibility and the CSP control responsibility. Controls that are MAC responsibility shall be documented within the SSPP, noting the related CSP that the control text is documented for.*

2. *Perform periodic review of CSP risk management program to verify that the CSP is complying with security requirements. This review should be performed at least annually. Identified risks should be documented within the contractor risk assessment.*

3. *Monitor and track risks identified from the cloud service provider. Identified risks should be documented within the contractor risk assessment.*

4. *Patching of vulnerabilities should be addressed in accordance with CMS defined patching timelines as noted in section 3.10.*

3.14 – MAC ARS Control Parameter Tailoring

(Rev. 15.1; Issued: 07-17-25; Effective: 02-28-25; Implementation: 08-18-25)

Limited tailoring of certain MAC ARS control parameters is permissible. The MAC ARS contains controls that are required to be implemented, but within certain controls, parts of the control can be tailored to meet appropriate system requirements. For controls where specific parameters are not fully documented, an acknowledgement of the parameter or setting shall be documented in CFACTS within the control implementation section. Any tailoring is subject to review, evaluation and adjustment by CMS. *Notification of tailoring needs to be communicated with DMSSOO prior to CFACTS submission.*

3.15 - Data Loss Prevention

(Rev. 15)

Data protection for a Business Partner's environment is critical in ensuring the privacy and integrity of their information. Business Partners must have a comprehensive Data Loss Prevention (DLP) solution in place to provide comfort that data is not being exfiltrated from their environment. The DLP solution should also provide assurance that if unauthorized data exfiltration is identified, it is blocked, and the effects are mitigated. The implemented DLP solution must cover data in use (endpoints), data in transit (network), and data at rest (data storage). Several tools implemented for other MAC ARS controls, such as Malicious Code Protection (endpoints), Intrusion Detection System/Intrusion Protection System (network) and encryption (data storage) can be combined to form a DLP solution. Business partners shall maintain documentation to support the DLP solution including formally maintained policies and procedures for the tools, controls, and processes.

3.16 - Wireless Access Monitoring

(Rev. 15)

As outlined in the MAC ARS, wireless access to a MAC network is not allowed unless explicitly approved in accordance with AC-18. MAC ARS AC-18 also states that an organization must monitor for unauthorized wireless access. Business partners must have a program in place to fulfill this requirement and have associated policies and procedures outlining how the program is operated. The implementation must be capable of identifying unauthorized wireless devices or access points that could be providing access to the network. Monitoring activities should be performed on a periodic basis as needed, but at least quarterly to confirm that unauthorized wireless access does not exist and/or is removed. If wireless access to the environment has been appropriately approved, an accurate and formally maintained listing of approved access points must be maintained to perform effective monitoring. The approved wireless access point list should be reviewed during the monitoring process to capture necessary updates.

3.17 - Malicious Code Protection

(Rev. 15.1; Issued: 07-17-25; Effective: 02-28-25; Implementation: 08-18-25)

MAC ARS requires that malicious code protection mechanisms be in place for an organization's information systems. If malicious code protection mechanisms are available for a system, they should be implemented and meet the requirements outlined in SI-3. If the solution in place provides malicious code protection sufficient to protect the device, however, cannot perform traditional file scanning based on the timing specified within SI-3 (e.g. AI solutions that rely on real time analysis), documentation should be maintained to demonstrate how the solution meets the security need of identifying malicious files in place of defined scanning times. In the event that an information system/platform does not have compliant malicious code protection mechanisms available for implementation, the Business Partner should put in place mitigating controls (e.g. file integrity monitoring) to assist in detecting/blocking the risk of malicious code. Documentation for these mitigating controls should be represented in formally maintained policies and procedures specific to the information systems in question.

3.18 *– Authorized Software*

(Rev. 15.1; Issued: 07-17-25; Effective: 02-28-25; Implementation: 08-18-25)

MAC ARS CM-7(5) requires that defined software be documented and explicitly authorized to be allowed to be executed. This authorization of software is known as whitelisting. If the whitelisting of software is a manual process, then the process to review and update the list of authorized software programs must be completed no less often than every seventy-two (72) hours. If automated tools are used to whitelist software, then the automated tools must be updated whenever the authorized software changes or new software is authorized, and the tool must be programmed to either perform a scan of the network for unauthorized software no less often than every seventy-two (72) hours or perform an on-demand evaluation of software every time the software is executed. In addition, management must review and formally document the list of approved software every 90 days.

3.19 – Data Encryption

(Rev. 15)

The MAC ARS includes several controls that require data encryption; however, the language included in some of the controls appears to conflict with language in other controls. To consistently address all of the data encryption controls included in the MAC ARS, for data that is not already encrypted at rest or in transit, a risk assessment shall be completed to determine if the CIA of the data can be maintained with or without encryption. All workstations and portable media containing PII or PHI should already be encrypted. For other hardware and software maintained within the documented and approved system security boundary, where the risk assessment determines that CIA is at risk, FIPS 140-2 compliant encryption shall be implemented for data in transit and/or data at rest. If the risk assessment determines that adequate controls are in place to protect the CIA of the data while it is within the documented and approved system security boundary, then the data can be transmitted and stored in the clear. Also, when encrypting data, the method of encryption can be determined to be hardware or software as appropriate.

3.20 – Firewall Ruleset Reviews

(Rev. 15.1; Issued: 07-17-25; Effective: 02-28-25; Implementation: 08-18-25)

Firewalls are key to preventing unauthorized and unwanted network traffic from entering or exiting a network and for restricting network access as a means of enforcing least privilege access. Firewalls accomplish this *by* using rulesets that determine which traffic is allowed to pass. The CMS TRA requires firewalls to functionally separate internal network zones.
In accordance with the latest revision of NIST Special Publication 800-41, management shall develop policies and procedures to periodically review firewall rulesets*/configurations* (both internal and external facing) to ensure they remain *compliant.* Management should use a risk-based approach for determining the frequency of the review for each firewall, but at a minimum, on a yearly basis. Areas to address in the policies and procedures include, but are not limited to:

- Validating old or out-of-date rules are prevented from processing by commenting them out or deleting them. Validating redundant rules are not active.
- Reviewing all rulesets*/configurations* to identify that change documentation or reference information that describes the purpose are documented. Management should be able to provide business justification for each active rule.
- Testing that changes do not break or bypass existing rulesets and function as intended.
- Documenting change management processes to confirm that rule changes were reviewed, tested, and approved.
- Comparing current rulesets to secured backups to validate that no unauthorized changes have occurred.
- Verifying known insecure protocols and potentially unnecessary IP addresses are being restricted.

If MACs decide to automate their Firewall rulesets review, they should ensure the following are *included, at minimum:*

- *Identification of redundant, duplicate, and conflicting rules.*
- *Identification of overly permissive rules.*
- *Identification of insecure ports and protocols.*
- *Identification of rules that are no longer used.*

Firewall ruleset reviews need to be documented and evidence of review maintained. The following types of information are important to maintain with the evidence of review:

- *Evidence of reports and/or documentation reviewed.*
- *Who reviewed the report and/or documentation, the result of the review, and when the review was performed.*
- *Tickets or documentation generated for addressing issues identified.*

3.21 – Artificial Intelligence (AI)

(Rev. 15.1; Issued: 07-17-25; Effective: 02-28-25; Implementation: 08-18-25)

There are operational and security focused tools that are changing the paradigm to increase staff efficiency and look at issues in a different way. While many of the new tools have useful new features, FISMA systems are required to follow the MAC ARS or demonstrate how the intent of the MAC ARS is being met. If an AI based tool is planned for use, then the security team needs to evaluate and document how the tool implements the MAC ARS. In addition, the following points need to be considered with implementing and maintaining an AI based solution.

- Potential issues with AI – There is often no audit trail, or supporting data, to show how the software arrived at its conclusion. Depending on the nature of a decision, supporting documentation may be needed to demonstrate how the decision was made.
- Periodic validation is required – Policies and procedures for periodic validation will need to be documented to make certain the tool is operating as intended and no security "gaps" exist. These will need to include instructions for recreating the results. If it is impossible to recreate the AI results with 100% accuracy, then tolerances need to be documented.
- Periodic assessment is required – Certain data may be used to initially seed the AI, but as conditions change, additional data may need to be added, or some data may need to be removed or modified. As changes are made, associated policies and procedures may need to be updated.
- AI account management – AI tools may bring complexity with accounts needed to operate effectively. Management should treat any account, even those used for AI, with the same security requirements as their other user, service, and administrative accounts.
- AI external connections – AI tools should be evaluated to determine if the tool operation or the data being analyzed is being sent outside of the organization-controlled network (e.g. cloud repository). If so, CMS should be consulted prior to implementation.
- In the event that the AI tool being implemented cannot align exactly to part of a MAC ARS control, management should evaluate if the tool has addressed the risk of the requirement. If the tool addresses the risk but the implementation is different than what the MAC ARS identifies, this should be documented within the organizations *SSPP* and policies. If the tool does not address the risk, then management may need to determine if additional control implementations are needed to fully address that MAC ARS control. MACs should consult with CMS if a technical limitation is encountered.

Additional information about AI at CMS can be found here: https://ai.cms.gov/.

4 - Information And Information Systems Security

(Rev. 15.1; Issued: 07-17-25; Effective: 02-28-25; Implementation: 08-18-25)

4.1 - Sensitive Information Protection Requirement

Business partners are responsible for implementing 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.

4.1.1 - Restricted Area

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 *business partner* 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 sign the register, providing 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.

4.1.2 - Security Room

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.

4.1.3 - Secured Area (Secured Interior/Secured Perimeter)

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 *shall* not *be* 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 *controls* 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.

4.1.4 - Container

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). *Acceptable*

containers for providing protection can be grouped into three general categories: locked containers, security containers, and safes or vaults.

4.1.4.1 - Locked Container

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.

4.1.4.2 - Security Container

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.

4.1.4.3 - Safe/Vault

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.

4.1.5 - Locking System

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.

4.1.6 - Physical Intrusion Detection System (IDS)

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 *after-hours* 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.

4.1.7 - Minimum Protection Alternatives
(Rev. 15)

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

4.2 - Encryption Requirements for Data Leaving Data Centers

(Rev. 15)

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.

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 in accordance with CMS standards. The only exception to this requirement is for hardcopy records that are transported to and from an off-site location and between off-site locations. To qualify for this exception, the controls listed below (additional information is available from CMS) shall be used.

To prepare the records for shipment:

- The records shall be stored in boxes.
- Each box shall be uniquely identified.
- Boxes shall be secured for shipment.
- Secured boxes shall be loaded into the shipping container or vehicle.
- Total items in each shipment shall be noted and the Bill of Lading signed.
- At time of pickup, the shipping company representative shall verify and sign the Bill of Lading.
- A copy of the identification records shall accompany each shipment.
- The shipping container or vehicle shall be locked and sealed with the seal number noted on the Bill of Lading.
- A copy of the completed Bill of Lading shall be kept by the contractor.

Upon receipt of the shipment at the storage facility:

- A storage facility representative shall verify the seal number and that it is unbroken.
- Compare the contents of the shipment against the Bill of Lading and the boxes against the copy of the identification record.
- If any discrepancies are found, the discrepancy shall be immediately resolved.
- After verification that all boxes shipped were received, information from the Bill of Lading shall be sent to the shipper where it shall be verified.
- Within 24 hours, all boxes on each shipment shall be scanned into the storage facility's tracking system and inserted into the storage racks.

5 – Secure Use of the Internet

(Rev. 15.1; Issued: 07-17-25; Effective: 02-28-25; Implementation: 08-18-25)

With prior written approval of their sponsoring CMS Business Owner, business partners may use the Internet for transmission of and/or receipt of health care transactions. Each request for using the Internet to conduct CMS business functions 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) assessment of security controls of the new functionality prior to its release into production is required and the assessment must include penetration testing. The assessment must be conducted to validate compliance with the following specific architectural, security, data interchange, and privacy requirements, as well as the MAC ARS. The existing requirement for an annual penetration test of the contractor network shall include any approved Internet infrastructure within the FISMA boundary. Compliance with existing MAC ARS requirements to conduct vulnerability scans and 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 the CMS Technical Reference Architecture (TRA), as currently released, and all its appendices.
    - 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, *CMS* Data Centers, and Standard Front-End initiatives.

2. Security:

    - Full compliance with the CMS Target Life Cycle Framework (Checkpoints, Deliverables, and Activities including Security Authorization) when introducing the new functionality.
    - Satisfactory systems test and evaluation of the Internet application to include evaluation of all applicable controls in the MAC ARS.
    - Compliance with DHHS and CMS standard configuration settings.
    - Compliance with the *current versions of* NIST SP 800-41, Guidelines on Firewalls and Firewall Policy; NIST SP 800-44, Guidelines on Securing Public Web Servers; NIST SP 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS) NIST 800-111, Guide to Storage Encryption Technologies for End User Devices; NIST SP 800-113, Guide to SSL VPNs; NIST SP 800-114, User's Guide to Securing External Devices for Telework and Remote Access; NIST SP 800-115, Technical Guide to Information Security Testing and Assessment; NIST SP 800-119, Guidelines for the Secure Development of IPv6; and NIST SP 800-144, Guidelines on Security and Privacy in Public Cloud Computing.
    - Security Authorization dependent on compliance with security control requirements and completion of documentation such as the ISRA, the security *and privacy* plan for the infrastructure, platform, and applications supporting the Internet functionality, and a CP for the supporting platform and application. *Authentication details shall be documented in accordance with CFACTS requirements.* All security documentation must be developed to the CMS methodologies and procedures provided at: *https://security.cms.gov/*.

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

4. Data Interchange *Standards*:

   - 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:

- A proof of concept/concept of operation paper describing the new application and functionality.
- Information that the Internet service shall be extended only to entities or providers enrolled in the jurisdiction of the proposing business partner.
- *If* the applicant has had a similar private side application*, they* shall describe the experience 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 MAC ARS controls. An application for these uses is not required. If not already in place, 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 Internet for these purposes.

References

(Rev. 15.1; Issued: 07-17-25; Effective: 02-28-25; Implementation: 08-18-25)

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

- CMS Information Security Library - *https://security.cms.gov/*
- NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems, May 2010.
  https://www.nist.gov/privacy-framework/nist-sp-800-34
- 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
- Federal Information System Controls Audit Manual (FISCAM), Exposure Draft, GAO-08-1029G, Section 3.5.
  https://www.gao.gov/products/gao-23-104975
- OMB Circular No. A-123, Management's Responsibility for Internal Control, Revised,
  https://www.whitehouse.gov/omb/information-for-agencies/circulars/
- Office of Management & Budget, Circular No. A-130, Appendix III, Security of Federal Automated Information Resources, 8 February 1996.
  https://www.whitehouse.gov/omb/information-for-agencies/circulars/

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

(Rev. 15)

Table of Contents

1 Introduction

(Rev. 15.1; Issued: 07-17-25; Effective: 02-28-25; Implementation: 08-18-25)

CMS business partners are required by the MAC ARS Contingency Planning family to develop and maintain *an* ITSCP. Business partners are expected to develop and test contingency plans that address key recovery scenarios that could occur as the result of a disastrous situation. While a contingency plan cannot address all possible scenarios, the plan should be structured to be useful in a variety of situations. When developing an ITSCP, the business partners are required to address all of the MAC ARS controls. The ITSCP needs to be developed in accordance with the CMS RMH Chapter 6 Contingency Planning document. In addition, *the current version of* NIST Special Publication 800-34, Contingency Planning Guide for Federal Information Systems, should be reviewed. NIST identifies different components and plan types that should be documented and be incorporated in a robust ITSCP.

The purpose of this appendix is to supplement the CMS RMH manual and NIST publication and 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. 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 ITSCP or updating an existing plan. In addition, the business partner's *SSPP* and ISRA should be used as a checkpoint to determine if appropriate contingencies have been addressed in the ITSCP. Also, the ITSCP should be coordinated with the Incident Response activities to address the restoration and recovery activities associated with an incident.

It can be noted that an ITSCP can be out of date shortly after it is created and updated. Automated tools exist to facilitate the development and maintenance of a plan. These tools can significantly help keep a plan current, but they may not address all the areas required, and they may not format the data in a manner that is consistent with CMS requirements. In these situations, the business partner will need to supplement the tools with additional information and cross references to ensure that all required information is documented.

2 Scope

(Rev. 15)

The business partner ITSCPs 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 ITSCP

(Rev. 15.1; Issued: 07-17-25; Effective: 02-28-25; Implementation: 08-18-25)

An ITSCP is a document that describes how to deal with an emergency or system disruption. These situations could be caused by, but not be limited to, a power outage, hardware failure, fire, or terrorist activity. An ITSCP 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.

Before developing an ITSCP, it is *required* to have or create 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 ITSCP 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 subjective argument relative to what constitutes an acceptable ITSCP. In this document, the description of an acceptable ITSCP 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 ITSCPs and test reports.

The following summary statements define what constitutes an acceptable ITSCP. 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.

2. The backup, recovery, and restoration of critical business functions, protecting equipment and data, and preserving the business reputation for providing high-quality service.

3. Is logical, reasonable, understandable, user friendly, and can be implemented under adverse circumstances.

4. Considers risk assessment results.

5. Addresses possible and probable emergencies or system disruptions that would require the implementation of the ITSCP.

6. Can be sufficiently tested on an established regular basis within recommended recovery periods at reasonable cost.

7. Contains information that is needed and useful during an emergency or system disruption.

8. Can, when implemented, produce a response and recovery, such that critical business functions are continued.

9. Specifies the *personnel* necessary to implement the plan, and clearly defines their responsibilities.

10. Clearly defines the resources necessary to implement the plan.

11. Reflects what can be done – is not a wish list.

12. Assumes people shall use sound judgment, but will need clearly stated guidance, since they will be functioning in *an unfamiliar* environment, under possibly severe conditions and pressure.

13. Addresses backup and alternate sites.

14. Addresses the use of manual operations, where appropriate and necessary.

15. Contains definitive "Call Lists" to use for contacting the appropriate persons in the proper sequence. These lists would include vendor points of contact.

An acceptable ITSCP should be concise. 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 ITSCP should serve as a "user's manual" and be easy to understand and use.

Because an ITSCP 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 an ITSCP 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.

Careful thought should be given to the organization of the ITSCP. 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 ITSCP. Not every informational item to be utilized during a contingency event will be in the ITSCP document. For example, the plan may point to an attachment or to a separate *procedure* manual. It is imperative to assure that any information provided in a separate *procedure* manual is readily available, easily obtainable and searchable.

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 IT Systems Contingency Planning

(Rev. 15)

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

4.1 Contingency Planning *(CP)*

(Rev. 15.1; Issued: 07-17-25; Effective: 02-28-25; Implementation: 08-18-25)

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 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 an IT systems contingency planning team. This team would be responsible for defining critical 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. 15)

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 address 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 IT Systems Contingency Plan

(Rev. 15.1; Issued: 07-17-25; Effective: 02-28-25; Implementation: 08-18-25)

The following required content, in conjunction with the format contained in the CMS RMH, may be used in developing an IT Systems CP. 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:
   - Scope

     Are the boundaries of the plan indicated? What organizations are involved, not involved?
     - Organizations
     - Systems
     - Boundaries
     - External Interfaces

   - 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 *units? A* CP shall address any standalone *units* 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 *organization(s)* does the CP apply?

    - Systems
      Is there a general description of systems and/or processes?

    - Boundaries
      Are the system boundaries clearly defined?

    - External Interfaces
      Are external interfaces clearly defined?

5. Three phases defined
   Does the plan address three phases of emergency or system disruption?

    - *Notification*
        - Is this phase adequately described so that it is understood what activities occur therein?
        - Are people, and their safety, considered?
        - 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?
    - Are effective recovery strategies in place for hardware, software, and data?
    - Are hardware configuration and operating system requirements considered?
    - Have interdependencies between internal and/or external systems considered?

- Restore/Reconstitute
    - Is this phase adequately described so that it is understood what activities occur during this phase?
    - Has validation of data been documented?
    - Has a clear path for validating system functionality and operational capabilities been implemented?

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?

    - Has a list of critical operations, data, and applications been created? In preparing the CP, a list of current critical operations, data and applications shall be documented and approved by management. This list shall contain the items needed to continue the minimum critical business elements and 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 within every 365 days? The CP shall be reviewed and tested under conditions as close to an emergency as can be reasonably and economically simulated.
        - Is there a provision for updating the CP within every 365 days?
        - Is the CP revised after testing, depending on test results? Are lessons learned documented and incorporated into the revise CP?

13. Relationships/Interfaces
    - Does the CP identify critical interfaces? Interfaces required to continue critical business functions should be identified. Refer to the System Security *and Privacy* 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?

    - 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 operations?
  - 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?

O. 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. 15)

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 within every 365 days 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 *Third Party* Data Centers (*TPDC*)

(Rev. 15.1; Issued: 07-17-25; Effective: 02-28-25; Implementation: 08-18-25)

Some contractors with which CMS has direct contracts do not have their own data centers. 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 that addresses the requirements outlined in the Appendix.

6.2 Multiple Contractors

(Rev. 15.1; Issued: 07-17-25; Effective: 02-28-25; Implementation: 08-18-25)

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

It is important to test a CP with a data center that serves multiple contractors. This provides an opportunity for the business partner to validate that they can recover the connection with the *TPDCs* to process claims.

6.3 Test Types

(Rev. 15)

CP test guidance suggests four types of testing:

- Walkthrough/Tabletop Test
- Checklists
- Simulation/modeling
- Live/Comprehensive Exercises

These are defined below:

- **Walkthrough/Tabletop Test**: 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.

  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.

- **Checklists**: Checklists are used to clearly present a step-by-step logical sequence so systems and sub-systems may be recovered in a logical manner. Checklists are intended to provide a direct, simple coordinated listing of events that ensure that all necessary steps are executed during the recovery process.

- **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.

- **Live/Comprehensive Exercises**: 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. 15)

- 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.

- Consider what a walkthrough test would miss.

- Consider the risks of missing that part of the test.

- Remember that there is risk in not doing a live test—is the risk acceptable?
  - 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 outweighs 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. 15.1; Issued: 07-17-25; Effective: 02-28-25; Implementation: 08-18-25)

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.

- End-to-end testing provides the best assurance that there are no problems.

- If the overall process to be tested can be sub-divided into critical and non-critical components, then only the critical components 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

- 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.

- 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 possible connections to help ensure minimum problems.
  - Or do simulation/modeling
  - Or do *a* walkthrough

Overall, end-to-end testing may combine walkthroughs, simulation/modeling, and live testing of contingencies. Walkthroughs and simulations may be used for non-critical systems, whereas critical systems shall be functionally tested under conditions that reproduce 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.

6.4 Test Planning

(Rev. 15)

An ITSCP 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
- After Action Report
- Retest
- Approvals

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

Following testing, any corrections specified in an After Action Report shall be included in the next ITSCP test. 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 ITSCP testing are formally discussed among senior business partner management, operations, IT management and staff, and the SSO.

Documentation shall exist for:

- Test plans
- Test results
- After Action Report
- Retest plans
- Memos of Understanding/Formal Test Arrangements
- Lessons Learned

7 Maximum Tolerable Downtime (MTD)

(Rev. 15)

MTD is the time it takes to recover an operation, function, process, program, file, or whatever has to be recovered as an operational entity. If claims processing operations must be recovered within 72 hours, then that is the MTD to recover. Anything over that is unacceptable.

- Recovery times may vary, depending on the criticality of the function 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 major function (e.g., claims processing, medical review, check generation).
- Recovery times shall be clearly defined and must be achievable.

8 Responsibilities

(Rev. 15)

Following is a summary of responsibilities for key groups and persons involved with developing business partner ITSCP.

8.1 Business Partner Management

(Rev. 15)

- Defines scope and purpose of IT systems contingency planning.
- Authorizes preliminary ITSCP planning.
- Ensures that appropriate ITSCPs are developed, periodically tested, and maintained.
- Ensures that all IT operations participate in the planning and development of the ITSCP.
- Reviews the ITSCP and documented recommendations.
- Requests and/or allocates funds for plan development and approved recommendations.
- Assigns teams to accomplish development of test procedures, and for testing the ITSCP.
- Reviews test results and document an After Action Report.
- Ensures that the appropriate personnel have been delegated and notified about 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 ITSCP
  - Changes to the ITSCP
  - Test plans
  - Test results
  - Corrective action management processes
  - Retest plans
  - Memos of Understanding/Formal Arrangement Documents
  - After Action Report
  - Changes to storage and backup/alternate site facilities

8.2 Systems Security Officer (SSO)

(Rev. 15)

- Documents the scope and purpose of ITSCP
- Reconciles discrepancies and conflicts in the ITSCP
- Evaluates security of backup and alternate sites
- Leads the preparation of the ITSCP
- Submits the ITSCP and recommendations to Business Partner Management
- Monitors implementation of the ITSCP and reports status to Business Partner Management
- Ensures all testing of the ITSCP is performed in accordance with CMS requirements
- Reviews test results
- Ensures that the ITSCP is updated based on test results
- Ensures lessons learned are discussed and formally documented in an After Action Report

- Obtains approval from the CMS Business Owner

9 ITSCP Changes

(Rev. 15)

The ITSCP shall be reviewed/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

9.1 ITSCP Attachments

(Rev. 15)

Materials that are too extensive to be included in the body of the Medicare ITSCP shall be included as attachments. These shall be kept current and referenced in the ITSCP. All attachments shall be available to appropriate ITSCP personnel. These shall also be a part of the System Security Profile. 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 ITSCP

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

(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. 15)

The following safeguards are specific countermeasures against fraudulent acts by employees whose functions involve Medicare program funds. These safeguards are consistent with the MAC ARS, 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?