Centers for Medicare & Medicaid Services
Information Security and Privacy Group

Risk Management Handbook (RMH)
Chapter 09: Maintenance

Final

Version 1.0

April 7, 2020

Record of Changes

The table below capture changes when updating the document. All columns are mandatory.

Version Number	Date	Chapter Section	Author/Owner Name	Description of Change
1.0	*01/032019*	*All*	*ISPG*	*Initial Version*

Effective Date/Approval

This Procedure becomes effective on the date that CMS's Director, Division of Security and Privacy Policy and Governance (DSPPG) signs it and remains in effect until it is rescinded, modified or superseded.

Signature: Michael E. Pagels -S Digitally signed by Michael E. Pagels -S Date: 2020.04.07 14:03:03 -04'00' Date of Issuance _____

Michael Pagels
Director, Division of Security and
Privacy Policy and Governance (DSPPG)
and Acting Senior Official for Privacy

Table of Contents

Tables

Figures

1. Executive Summary

The controls listed in this chapter focus on how the organization must perform periodic and timely maintenance on organizational information systems and provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

2. Introduction

2.1 Purpose

The Centers for Medicare & Medicaid Services (CMS) Risk Management Handbook (RMH) Chapter 9 Maintenance provides the procedures for implementing the requirements of the CMS Information Systems Security and Privacy Policy (IS2P2) and the CMS Acceptable Risk Safeguards (ARS). The following is a diagram that breaks down the hierarchy of the IS2P2, ARS, and RMH:

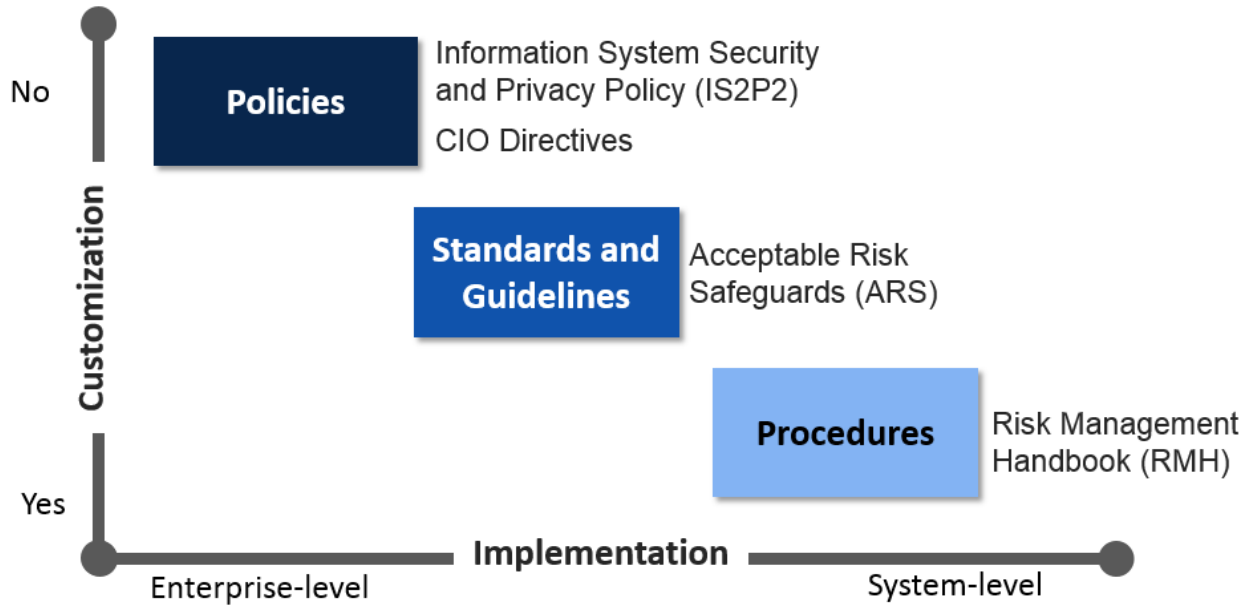

Figure 1: Hierarchy of IS2P2, ARS and RMH

This document describes procedures that facilitate the implementation of security controls associated with the Maintenance (MA) family of controls. To promote consistency among all RMH Chapters, CMS intends for Chapter 9 to align with guidance from the National Institute of Standards and Technology (NIST), tailoring that content to the CMS environment.

2.2 Authority

The Federal Information Security Management Act (FISMA) requires each federal agency to develop, document and implement an agency-wide program to provide information security for the information and systems that support the operations and assets of the agency, including those provided or managed by another agency or contractor. The Federal Information Security

Modernization Act of 2014 designates NIST with responsibility to develop guidance to federal agencies on information security and privacy requirements for federal information systems.

As an operating division of the Department of Health and Human Services (HHS), CMS must also comply with the HHS IS2P, Privacy Act of 1974 ("Privacy Act"), the Privacy and Security Rules developed pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and the E-Government Act of 2002, which relates specifically to electronic authentication requirements. The HHS Office for Civil Rights (OCR) is responsible for enforcement of the HIPAA Security and Privacy Rules. CMS seeks to comply with the requirements of these authorities, and to specify how CMS implements compliance in the CMS IS2P2.

HHS and CMS governance documents establish roles and responsibilities for addressing privacy and security requirements. In compliance with the HHS Information Systems Security and Privacy Policy (IS2P), the CMS Chief Information Officer (CIO) designates the CMS Chief Information Security Officer (CISO) as the CMS authority for implementing the CMS-wide information security program. HHS also designates the CMS Senior Official for Privacy (SOP) as the CMS authority for implementing the CMS-wide privacy program. Through their authority given by HHS, the CIO and SOP delegate authority and responsibility to specific organizations and officials within CMS to develop and administer defined aspects of the CMS Information Security and Privacy Program.

All CMS stakeholders must comply with and support the policies and the procedures referenced in this handbook to ensure compliance with federal requirements for implementation of information security and privacy controls.

2.3 Scope

This handbook documents procedures that facilitate the implementation of the privacy and security controls defined in the CMS IS2P2 and the CMS ARS. This RMH Chapter provides authoritative guidance on matters related to the Maintenance family of controls for use by CMS employees and contractors that support the development, operations, maintenance, and disposal of CMS information systems.

Security control inheritance is a situation in which an information system or application receives protection from security controls or portions of security controls that are developed, implemented, and assessed, authorized, and monitored by entities other than those responsible for the system or application. Security controls most often offered up for inheritance are in the Physical and Environmental Protection (PE), Media Protection (MP) and Maintenance (MA) families. The MA controls listed in this RMH provide a typical example of inheritance for an information system hosted within a CMS data center.

This handbook does not supersede any applicable laws, existing labor management agreements, and/or higher-level agency directives or other governance documents.

2.4 Background

This handbook aligns with NIST SP 800-53 catalogue of controls, the CMS IS2P2, and the CMS ARS. Each procedure relates to a specific NIST security control family. Additional sections of this

document crosswalk requirements to other control families and address specific audit requirements issued by various sources (e.g., OMB, OIG, HHS, etc.).

RMH Chapter 09 provides processes and procedures to assist with the consistent implementation of the MA family of controls for any system that stores, processes, or transmits CMS information on behalf of CMS. This chapter identifies the policies, minimum standards, and procedures for the effective implementation of selected security and privacy controls and control enhancements in the MA family.

CMS's comprehensive information security and privacy policy framework includes:

- An overarching policy (CMS IS2P2) that provides the foundation for the security and privacy principles and establishes the enforcement of rules that will govern the program and form the basis of the risk management framework
- Standards (CMS ARS) that address specific information security and privacy requirements
- Procedures (RMH series) that assist in the implementation of the required security and privacy controls based upon the CMS ARS standards.

FISMA further emphasizes the importance of continuously monitoring information system security by requiring agencies to conduct assessments of security controls at a risk-defined frequency. NIST SP 800-53 states that an organization must define, develop, disseminate, review, and update its documentation at least once every three years. This includes a formal, documented system security package that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and formal, documented processes and procedures to facilitate the implementation of the policy and associated controls.

The Risk Assessment process exists within the Risk Management Framework (RMF) which emphasizes:

- Building information security capabilities into federal information systems through the application of state-of-the-practice management, operational, and technical security controls
- Maintaining awareness of the security state of information systems on an ongoing basis though enhanced monitoring processes
- Providing essential information to senior leaders to facilitate decisions regarding the mitigation or acceptance of information-systems-related risk to organizational operations and assets, individuals, external organizations, and the Nation.

The RMF[1] has the following characteristics:

- Promotes the concept of near-real-time risk management and ongoing-information-system authorization through the implementation of robust continuous monitoring processes;

[1] https://csrc.nist.gov/publications/detail/sp/800-37/rev-1/final

- Encourages the use of automation to provide senior leaders the necessary information to make cost-effective, risk-based decisions with regard to the organizational information systems supporting their core missions and business functions;
- Integrates information security and privacy protections into the enterprise architecture and CMS Defined System Development Life Cycle (CMS-SDLC)
- Provides guidance on the selection, implementation, assessment, and monitoring of controls and the authorization of information systems;
- Links risk management processes at the information system level to risk management processes at the organization level through a risk executive (function); and
- Establishes responsibility and accountability for security and privacy controls deployed within organizational information systems and inherited by those systems (i.e., common controls).

3. Policy

Policy delineates the security management structure, clearly assigns security responsibilities, and lays the foundation necessary to reliably measure progress, compliance, and direction to all CMS employees, contractors, and any individual who receives authorization to access CMS information technology (IT) systems or systems maintained on behalf of CMS to assure the confidentiality, integrity, and availability of CMS information and information systems.

3.1 Information Systems Security and Privacy Policy (IS2P2)

The CMS IS2P2[2] defines the framework and policy under which CMS protects and controls access to CMS information and information systems in compliance with HHS policy, federal law, and regulations. This Policy requires all CMS stakeholders to implement adequate information security and privacy safeguards to protect all CMS sensitive information.

The policy contained within the CMS IS2P2 and the procedures contained within this document assist in satisfying the requirements for controls that require CMS to create a policy and associated procedures related to information systems.

3.2 Chief Information Officer (CIO) Directives

The CMS Chief Information Officer (CIO), the CMS Chief Information Security Officer (CISO), and the CMS Senior Official for Privacy (SOP) jointly develop and maintain the CMS IS2P2. The CIO delegates authority and responsibility to specific organizations and officials within CMS to

[2] https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/CMS-Information-Systems-Security-and-Privacy-Policy-IS2P2.html?DLPage=1&DLEntries=10&DLFilter=is2&DLSort=0&DLSortDir=ascending

develop and administer defined aspects of the CMS Information Security and Privacy Program as appropriate.

The dynamic nature of information security and privacy disciplines and the constant need for assessing risk across the CMS environment can cause gaps in policy, to arise outside of the policy review cycle. The CMS Policy Framework includes the option to issue a CIO Directive[3] to address identified gaps in CMS policy and instruction to provide immediate guidance to CMS stakeholders while a policy is being developed, updated, cleared, and approved.

4. Standards

Standards define both functional and assurance requirements within the CMS security and privacy environment. CMS policy is executed with the requirements prescribed in standards with the objective of enabling consistency across the CMS environment. The CMS environment includes users, networks, devices, all software, processes, information in storage or transit, applications, services, and systems that can be connected directly or indirectly to networks. These components are responsible for meeting and complying with the security and privacy baseline defined in policy and further prescribed in standards. The parameters and thresholds for policy implementation are built into the CMS standards, and provide a foundation for the procedural guidance provided by the Risk Management Handbook series.

4.1 Acceptable Risk Safeguards (ARS)

The CMS Acceptable Risk Safeguards (ARS)[4] provides the minimum acceptable level of required security and privacy controls that must be implemented to protect CMS's information and information systems, including CMS sensitive information. The initial selection of the appropriate controls is based on control baselines. The initial control baseline is the minimum list of controls required for safeguarding an IT system based on the organizationally identified needs for confidentiality, integrity, and/or availability.

A different baseline exists for each security category (high, moderate, low) as defined by NIST Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems. The ARS provides a catalog of low, moderate, and high controls, in addition to non-mandatory controls outside of the FIPS-199 baseline selection. The ARS, based upon the FIPS 200 and NIST SP 800-53, provides guidance on tailoring controls and enhancements for specific types of missions and business functions, technologies, or environments of operation. Users of the ARS may tailor specific mandatory controls as well as most of the non-mandatory and unselected controls.

[3] https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/CIO-Directives-and-Policies/Policies.html

[4] https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/ARS-31-Publication.html?DLPage=1&DLEntries=10&DLSort=0&DLSortDir=ascending

5. HIPAA Integration

The HIPAA Security Rule is designed to be flexible, scalable, and technology neutral, which enables it to be adaptive and seamlessly integrated with detailed frameworks such as FISMA. Although both regulations are governed by different federal agencies, the HIPAA Security Rule only applies to covered entities and their business associates as defined within HIPAA. Implementation of the FISMA requirements helps achieve compliance with the HIPAA Security Rule. HIPAA provides guidance to address the provisions required for the security of health-related information, whereas FISMA presents instructions for the security of the information and the information systems that support these activities.

The table below shows a crosswalk mapping of security controls found in this RMH to specific sections and requirements found in HIPAA.

Table 1: Crosswalk- Mapping Controls to HIPAA Requirements

Maintenance (MA) Control	HIPAA Section
MA-2	§§ 164.308(a)(1)(ii)(D), 164.308(a)(3)(ii)(A), 164.310(a)(2)(iv), 164.312(b)
MA-3	§§ 164.308(a)(3)(ii)(A), 164.310(a)(2)(iv)
MA-4	§§ 164.308(a)(3)(ii)(A), 164.310(d)(1), 164.310(d)(2)(ii), 164.310(d)(2)(iii), 164.312(a), 164.312(a)(2)(ii), 164.312(a)(2)(iv), 164.312(b), 164.312(d), 164.312(e), 164.308(a)(1)(ii)(D)
MA-5	§§ 164.308(a)(3)(ii)(A), 164.310(a)(2)(iv)

6. Roles and Responsibilities

A comprehensive list of information security and privacy roles and responsibilities for CMS stakeholders is contained in the CMS IS2P2. The table below shows the roles from the CMS IS2P2 that are specific to the procedures contained within this RMH chapter.

Table 2: Roles and Responsibilities

Role	**Applicable Controls**
CMS Business Owner (BO)	MA-02
CMS Chief Information Officer (CIO)	MA-3(3)
CMS System Developer and Maintainer	MA-5

7. Common Control Inheritance

The inherited controls list can be used to identify common controls offered by system alternatives. The use of inherited controls is optional, the objective of this processes is to identify opportunities to extract benefits (and reduce costs) by maximizing the use of already existing solutions, and minimizing duplication of efforts across the enterprise. Below is a listing of controls that can be inherited, where they can be inherited from and if they are a hybrid control for this control family.

Table 3: Common Controls

Control	Inheritable From	Hybrid Control
MA-01	OCISO Inheritable Controls	Yes
MA-02	CMS Baltimore Data Center - EDC4	No
MA-02(02)	CMS Baltimore Data Center - EDC4	No
MA-03	CMS Baltimore Data Center - EDC4	No
MA-03(01)	CMS Baltimore Data Center - EDC4	No
MA-03(02)	CMS Baltimore Data Center - EDC4	No
MA-03(03)	CMS Baltimore Data Center - EDC4	No
MA-04	CMS Baltimore Data Center - EDC4	No
MA-04(01)	CMS Baltimore Data Center - EDC4	No
MA-04(02)	CMS Baltimore Data Center - EDC4	No
MA-04(03)	CMS Baltimore Data Center - EDC4	No
MA-04(06)	CMS Baltimore Data Center - EDC4	No
MA-05	CMS Baltimore Data Center - EDC4	No
MA-05(01)	CMS Baltimore Data Center - EDC4	No
MA-06	CMS Baltimore Data Center - EDC4	No

8. Procedures

Procedures assist in the implementation of the required security and privacy controls. In this section, the Maintenance family of procedures is outlined. To increase traceability, this procedure maps to the associated NIST security controls using the corresponding control number from the CMS IS2P2.

7.1 Controlled Maintenance (MA-2)

This control addresses the information security aspects of the information system maintenance program and applies to all types of maintenance to any system component (including applications) conducted by any local or nonlocal entity (e.g., in-contract, warranty, in-house, software

maintenance agreement). System maintenance also includes those components not directly associated with information processing and/or data/information retention such as scanners, copiers, and printers.

The level of detail included in maintenance records can be informed by the security categories of organizational information systems. Organizations must consider supply chain issues associated with replacement components for information systems

Guidance for systems processing, storing, or transmitting PHI:

HIPAA requires organizations to apply reasonable and appropriate safeguards for the protection of PHI, including implementing policies and procedures to document repairs and modifications to the facility which are related to security.

The table below outlines the CMS defined parameters for MA-2.

Table 4: CMS Defined Parameters-Control MA-2

Control	Control Requirement	CMS Parameter
MA-2	The organization: c. Requires that [Assignment: organization-defined personnel or roles] explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs;	The organization: c. Requires that the applicable Business Owner (or an official designated in the applicable security plan) explicitly approves the removal of the information system or system components from organizational facilities for off-site maintenance or repairs;

CMS reviews and updates the baseline configuration[5] of its information systems at a regularly defined frequency, when special circumstances arise (e.g., critical security patches), or when an information system component is installed or upgraded. Automation assists in documenting changes and ensures the proper workflow. CMS uses automated means to document system changes for submission and to notify the authorizing personnel, defined in the System Security Plan (SSP), who are designated to approve changes, whenever changes are proposed. Automating these processes also increases the traceability of changes for many systems at once. RMH Chapter 05 Configuration Management[6] provides additional information on change management.

CMS addresses the information security aspects of the information system maintenance program and applies it to hardware and software maintenance. Information necessary for creating effective maintenance records includes, at a minimum, the following information:

- Date and time of maintenance;
- Name of individuals or group performing the maintenance;

[5] A Baseline Configuration is a set of specifications for a system that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures. The baseline configuration is used as a basis for future builds, releases, and/or changes.

[6] https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/RMH-Chapter-05-Configuration-Management.pdf

- Name of the authorized escort (if necessary);
- A description of the maintenance performed;
- A list of the information system components/equipment removed and/or replaced. **NOTE:** The removal of the information system or components from CMS facilities requires the explicit approval from the Business Owner (BO). Prior to off-site maintenance or repairs, the equipment is sanitized, using approved CMS sanitization methods, for the removal of information from associated media.

7.2 Maintenance Tools (MA-3)

This control addresses security-related issues associated with maintenance tools used specifically for diagnostic and repair actions on organizational information systems. Maintenance tools can include hardware, software, and firmware items. Maintenance tools are potential vehicles for transporting malicious code, either intentionally or unintentionally, into a facility and subsequently into organizational information systems. Maintenance tools can include hardware/software diagnostic test equipment and hardware/software packet sniffers. This control does not cover hardware/software components that may support information system maintenance, yet are considered an integral part of the system.

CMS approves, controls, and monitors information system maintenance tools that are used to repair or conduct diagnostics on information systems and their components. After completion of the maintenance, all maintenance equipment, with the capability of retaining information, is checked to ensure that information is not saved on the equipment and that the equipment is appropriately sanitized, using approved CMS sanitization methods[7], prior to the release from the CMS facility.

7.2.1 Inspect Tools (MA-3(1))

This control enhancement provides that maintenance tools, transported by maintenance personnel into facilities, are inspected for unauthorized modifications.

CMS inspects maintenance tools for obvious signs of improper or unauthorized modifications. Tools that are found to be modified in an improper or unauthorized manner must be reported per the CMS incident handling procedure that is located in RMH Chapter 08 Incident Response[8].

7.2.2 Inspect Media (MA-3(2))

Inspecting media that contains diagnostic and test programs for malicious code before the media are used in the information system is the purpose of this control enhancement.

[7] https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/RMH-Chapter-10-Media-Protection.pdf

[8] https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/RMH-Chapter-08-Incident-Response.pdf

CMS checks and scans all diagnostic tools and test programs for malicious code before being used in the information system. Media that are found to contain malicious code must be reported per the CMS incident handling procedure that is located in RMH Chapter 08 Incident Response[9].

7.2.3 Prevent Unauthorized Removal (MA-3(3))

Preventing the unauthorized removal of maintenance equipment containing organizational information is the purpose of this control enhancement.

The table below outlines the CMS defined parameters for MA-3(3).

Table 5: CMS Defined Parameters-Control MA-3(3)

Control	Control Requirement	CMS Parameter
MA-3(3)	The organization prevents the unauthorized removal of maintenance equipment containing organizational information by: d. Obtaining an exemption from [Assignment: organization-defined personnel or roles] explicitly authorizing removal of the equipment from the facility.	The organization prevents the unauthorized removal of maintenance equipment containing organizational information by: d. Obtaining an exemption, in writing, from the CMS CIO or his/her designated representative explicitly authorizing removal of the equipment from the facility.

CMS prevents the unauthorized removal of maintenance equipment containing organizational information by:

- Verifying that CMS information is not contained on the equipment when the equipment has the capability of retaining information;
- Sanitizing or destroying the equipment, using CMS approved sanitization or destruction techniques/methods[10]
- Retaining or storing the equipment securely within the facility;
- Obtaining a written exemption from the CMS Chief Information Officer (CIO), or his/her designated representative, explicitly authorizing removal of the equipment from the facility.

7.3 Nonlocal Maintenance (MA-4)

Nonlocal maintenance and diagnostic activities are those activities conducted by individuals communicating through a network, either an external network (e.g., the Internet) or an internal network. Local maintenance and diagnostic activities are those activities carried out by individuals physically present at the information system or information system component and not communicating across a network connection. Authentication techniques used in the establishment

[9] https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/RMH-Chapter-08-Incident-Response.pdf

[10] https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/RMH-Chapter-10-Media-Protection.pdf

of nonlocal maintenance and diagnostic sessions reflect the network access requirements in *Identification and Authentication (Organizational Users)* (*IA-2).*

Written authorization from the CMS CIO is required for nonlocal or remote maintenance and diagnostic activities to be performed on an information system. CMS monitors and controls nonlocal maintenance and diagnostic activities and allows the use of maintenance and diagnostic tools in accordance with organizational policy. Appropriate identification and authentication techniques are employed in the establishment of remote sessions in accordance with *IA-2*, and all such sessions are terminated after the completion of the maintenance.

7.3.1 Auditing and Review (MA-4(1))

The purpose of this control enhancement is to ensure that auditing and reviews of nonlocal maintenance and diagnostic sessions are performed.

Table 6: CMS Defined Parameters-Control MA-4(1)

Control	Control Requirement	CMS Parameter
MA-4(1)	The organization: a) Audits nonlocal maintenance and diagnostic sessions [Assignment: organization-defined audit events];	The organization: a. Audits nonlocal maintenance and diagnostic sessions using available audit events;

CMS audits nonlocal maintenance and diagnostic sessions using available audit events. Maintenance and diagnostic records consist of audit events that are a defined selection based on all events for which the information system is capable of generating records. CMS reviews these records on a continuous basis.

7.3.2 Document Nonlocal Maintenance (MA-4(2))

Information systems that require nonlocal maintenance must document the policies and procedures used for establishing and using nonlocal maintenance activities to include testing and diagnostic connection.

CMS requires that maintenance activity, including the authentication mechanism for granting remote access and the capture of maintenance information, is recorded in the applicable SSP.

7.3.3 Comparable Security/Sanitization (MA-4(3))

Comparable security capability on information systems, diagnostic tools, and equipment providing maintenance services implies that the implemented security controls on those systems, tools, and equipment are at least as comprehensive as the controls on the information system being serviced.

CMS requires that nonlocal maintenance and diagnostic services are performed from an information system that implements a security capability comparable to the capability implemented on the system being serviced. Prior to nonlocal maintenance or diagnostic services, CMS requires the removal the component to be serviced from the information system and sanitization of information from the component. After the service is performed and before

reconnecting the component to the information system, CMS provides for inspection and sanitization of the component for potentially malicious software.

7.4 Maintenance Personnel (MA-5)

This control applies to individuals performing hardware or software maintenance on organizational information systems, while *Physical Access Authorizations (PE-2)* addresses physical access for individuals whose maintenance duties place them within the physical protection perimeter of the systems.

Guidance for systems processing, storing, or transmitting PII (to include PHI):

If maintenance personnel are contractors, then the organizations personnel responsible for contracting (such as the contracting officer, contracting officer's representative, or contracting officer's technical representative or the program manager must ensure that contractors having access to records (i.e., files or data) from a system of records are contractually bound to be covered by the Privacy Act of 1974.

CMS maintains documentation of authorized maintenance personnel that perform hardware or software maintenance on information systems. The System Developer and Maintainer implements approved software maintenance while the Government Task Lead (GTL) of the data center maintains a list of authorized maintenance personnel that perform hardware maintenance.

Maintenance personnel performing hardware maintenance are required to have authorized physical access to the data center. RMH Chapter 11 Physical and Environmental Protection[11] provides additional information on requesting physical access to controlled areas.

7.4.1 Individuals Without Appropriate Access (MA-5(1))

This control enhancement denies visual and electronic access to any classified information, Controlled Unclassified Information (CUI), or any other sensitive information contained on organizational information systems to individuals who do not possess the required level of security clearances or who are not U.S. citizens.

Individuals not previously identified as authorized maintenance personnel, such as information technology manufacturers, vendors, systems integrators, and consultants, may require privileged access to CMS information systems when required to conduct maintenance activities with little or no notice. Maintenance personnel without the necessary access authorizations, clearances or formal approvals are properly escorted and supervised by an authorized CMS employee or an authorized contractor with technical competence of supervising individuals relating to the maintenance being performed on the information system.

7.5 Timely Maintenance (MA-6)

Organizations specify the information system components that result in increased risk to organizational operations and assets, individuals, other organizations, or the Nation when the

[11] https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/RMH-Chapter-11-Physical-and-Environmental-Protection.pdf

functionality provided by those components is not operational. Organizational actions to obtain maintenance support typically include having appropriate contracts in place.

The table below outlines the CMS defined parameters for MA-6.

Table 7: CMS Defined Parameters-Control MA-6

Control	Control Requirement	CMS Parameter
MA-6	The organization obtains maintenance support and/or spare parts for [Assignment: organization-defined information system components] within [Assignment: organization-defined time period] of failure.	The organization obtains maintenance support and/or spare parts for defined key information system components (defined in the applicable security plan) within the applicable RTO specified in the contingency plan.

CMS requires the alignment of hardware maintenance and support services with the information system's recovery time objective (RTO)[12]. Timely maintenance requirements are met through service agreements that provide 24/7 coverage and/or through on-site storage of replacement parts.

CSPs must define a list of security-critical information system components and/or key information technology components. The list of components is approved and accepted by the Joint Authorization Board (JAB). The time period to obtain maintenance and spare parts is defined in accordance with the contingency plan for the information system and business impact analysis. The time period is approved and accepted by the JAB.

[12] Recovery time objective (RTO) is the maximum desired length of time allowed between an unexpected failure or disaster and the resumption of normal operations and service levels.

Appendix A: Acronyms

Selected acronyms used in this document are defined below.

Acronyms	Terms
ARS	Acceptable Risk Safeguards
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CMS	Centers for Medicare & Medicaid Services
CMS IS2P2	CMS Information Systems Security and Privacy Policy
HHS	Health and Human Services
IR	Incident Response
ISPG	Information Security and Privacy Group
NIST	National Institute of Standards and Technology
ODP	Organizational Defined Parameters
RMH	Risk Management Handbook
SOP	Senior Official for Privacy
SP	Special Publication
URL	Universal Resource Locator
USB	Universal Serial Bus

Appendix B: Glossary of Terms

Selected terms found in this document are defined below.

Terms	Definitions
Acceptable Risk Safeguards	CMS Information Security Acceptable Risk Safeguards (ARS), CMS Minimum Security Requirements (CMSR)
Centers for Medicare & Medicaid Services	CMS covers 100 million people through Medicare, Medicaid, the Children's Health Insurance Program, and the Health Insurance Marketplace.
Chief Information Security Officer	The incumbent in the position entitled Chief Information Security Officer. The CISO must be an agency official (federal government employee) and must fulfill all of the responsibilities identified in the HHS IS2P Appendix A Section 11, OpDiv CISOs. The CISO carries out the CIO's information security responsibilities under federal requirements in conjunction with the SOP.
Information Systems Security and Privacy Policy	This Policy provides direction to all CMS employees, contractors, and any individual who receives authorization to access CMS information technology (IT) systems or systems maintained on behalf of CMS to assure the confidentiality, integrity, and availability of CMS information and systems. As the federal agency responsible for administering the Medicare, Medicaid, Children's Health Insurance Program (CHIP), and Health Insurance Marketplace (HIM); CMS collects, creates, uses, discloses, maintains, and stores personal, healthcare, and other sensitive information subject to federal law, regulation, and guidance.
Risk Management Handbook	The Risk Management Handbook (RMH) compiles CMS standards, requirements, directives, practices, and procedures for protecting CMS information and information systems.

Appendix C: Applicable Laws and Guidance

The Applicable Laws and Guidance appendix provides references to both authoritative and guidance documentation supporting the "document." Subsections are organized to "level of authority" (e.g., Statutes take precedence over Federal Directives and Policies).

C.1 Statutes

1 Health Insurance Portability and Accountability Act of 1996 (HIPAA)

http://www.hhs.gov/hipaa

C.2 Federal Directives and Policies

1 FedRAMP Rev. 4 Baseline

https://www.fedramp.gov/files/2015/03/FedRAMP-Control-Quick-Guide-Rev4-FINAL-01052015.pdf

C.3 NIST Guidance and Federal Information Processing Standards FIPS Pub: 140-2, 197, 201

1 FIPS-140-2 *Security Requirements for Cryptographic Modules*

https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf

2 FIPS-197, *Advanced Encryption Standard*

https://csrc.nist.gov/csrc/media/publications/fips/197/final/documents/fips-197.pdf

3 FIPS-201-2, *Personal Identity Verification (PIV) for Federal Employees and Contractors*

https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf

4 NIST SP 800-88, *Guidelines for Media Sanitization*

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-88.pdf

5 NIST SP 800 100, *Information Security Handbook: A Guide for Managers*

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-100.pdf

6 NIST SP 800 12 rev.1 *An Introduction to Information Security*

https://csrc.nist.gov/publications/detail/sp/800-12/rev-1/final

C.4 HHS Policy

1 HHS-OCIO-2014-0001 HHS Information System Security and Privacy Policy (HHS IS2P)

HHS Information Security and Privacy Policy (IS2P) – 2014 Edition. To obtain a copy of this document, please email fisma@hhs.gov

C.5 CMS Policy and Directives

1 *CMS Information Systems Security and Privacy Policy (IS2P2)*

https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/IS2P2.pdf

C.6 Associated CMS Resources

1 CMS Acceptable Risk Safeguards (ARS) 3.1

https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/ARS-31-Publication.html?DLPage=1&DLEntries=10&DLFilter=ars%203.1&DLSort=0&DLSortDir=ascending

Appendix D: Points of Contact

CMS IT Service Desk

Name	Email	Phone
CMS IT Service Desk	CMS_IT_Service_Desk@cms.hhs.gov	(410) 786-2580 (800) 562-1963

Appendix E: Feedback and Questions

Information security is a dynamic field and as such policies, standards, and procedures must be continually refined and updated. Feedback from the user community is invaluable and ensures accurate documentation. For any recommendations for improvements to this document or any questions about the material included within, please email the CISO mailbox at CISO@cms.hhs.gov. Your feedback will be evaluated for incorporation into future releases of the document.