WHITE PAPER

Migration from EDE to ARC-AMPE Maintenance (MA) controls

CMS requirements for Direct Enrollment Entities

JESSICA PAYNE, CONSULTANT
IAN WALTERS, PRINCIPAL

Table of contents

Purpose

This white paper provides a guide for Direct Enrollment Entities (DEEs) to upgrade their Enhanced Direct Enrollment (EDE) System Security and Privacy Plans (SSPPs) to the Acceptable Risk Controls for ACA, Medicaid, and Provider Entities (ARC-AMPE).

Due to the substantial number of controls, and to facilitate ease of use, this white paper is one of a series of 20 which divides the ARC-AMPE by control family. This white paper addresses the Maintenance controls.

ARC-AMPE Control Families

Control Family	Number of Controls
Access Control	46
Awareness and Training	9
Audit and Accountability	18
Assessment, Authorization, and Monitoring	12
Configuration Management	25
Contingency Planning	16
Identification and Authentication	21
Incident Response	15
Maintenance (This Document)	**12**
Media Protection	8
Physical and Environmental Protection	9
Planning	6
Program Management	5
Personnel Security	8
Personally Identifiable Information Processing and Transparency	10
Risk Assessment	8
System and Services Acquisition	18
System and Communications Protection	28
System and Information Integrity	30
Supply Chain Risk Management	4

Background

Affordable Care Act

The Affordable Care Act (ACA) revolutionized access to healthcare in the United States by establishing Health Insurance Marketplaces (HIMs). Enhanced Direct Enrollment (EDE) is an ACA innovation that allows third-party entities, such as insurers and web-brokers, to offer consumers a seamless application and enrollment experience directly through their platforms. This approach improves accessibility to the marketplace while maintaining compliance with federal regulations.

Enhanced Direct Enrollment

> *Direct Enrollment (DE) is a service that allows approved Qualified Health Plan (QHP) issuers and third-party web-brokers (online insurance sellers) to enroll consumers in Exchange coverage, with or without the assistance of an agent/broker, directly from their websites.*
>
> *The Enhanced Direct Enrollment (EDE) user experience goes well beyond the plan shopping and enrollment experience that is available via Classic DE. EDE is a service that allows approved EDE entities (e.g., QHP issuers and web-brokers approved to participate in EDE) to provide a comprehensive consumer experience including the eligibility application, Exchange enrollment, and post-enrollment year-round customer service capabilities for consumers and agents/brokers working on behalf of consumers, directly on issuer and web-broker websites. Through EDE, approved EDE Entities build and host a version of the HealthCare.gov eligibility application directly on their websites that securely integrates with a back-end suite of Federally Facilitated Exchanges (FFEs) application programing interfaces (APIs) to support application, enrollment and more.*
>
> Source: cms.gov

CMS oversight

The Centers for Medicare & Medicaid Services (CMS) exercises oversight of DEEs, which are responsible for overseeing and managing marketplace operations to ensure compliance with federal regulations, safeguard consumer data, and maintain the integrity of the HIM. Key aspects of CMS's oversight include:

- Requiring DEEs to undergo rigorous audit processes, including demonstrating compliance with security and privacy control requirements.
- Enforcing strict data protection measures in the DE environment to ensure the confidentiality, integrity, and availability of consumer data and requiring entities to implement cybersecurity controls, conduct regular risk assessments, and submit independent security audits.
- Requiring DEEs to adhere to operational policies and procedures, such as providing accurate plan information, maintaining transparent consumer interactions, and facilitating HIM enrollment without bias.
- Requiring DEEs to report any data breaches or system incidents promptly and to take corrective actions as directed by CMS and the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR).
- Requiring DEEs to renew their Authority to Connect (ATC) annually, providing updated documentation and evidence of continued compliance with all requirements.

Through these oversight mechanisms, CMS ensures that DEEs in the healthcare.gov environment deliver secure, compliant, and user-friendly services, aligning with the ACA's mission to expand access to quality health coverage.

ARC-AMPE

CMS published the ARC-AMPE for Direct Enrollment Entities (DEEs) Version 1.0 dated July 7th, 2025. This framework replaces the EDE security and privacy guidelines:

- ARC-AMPE Volume 1 contains high-level guidance, and Volume 2 has the minimum-level security and privacy controls.
- ARC-AMPE Volume 2 is the new format for the SSPP for DEEs.
- The compliance date for DEEs is June 2026.

The minimum control baseline for ARC-AMPE DEE compliance consists of 308 controls which have been derived from the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 5, “Security and Privacy Controls for Information Systems and Organizations.”

The number of controls required for the mandatory baseline represents a significant increase from the EDE baseline (295 controls), and DEEs should be prepared for an increased level of effort for developing the SSPP and submitting more artifacts during audits.

Another major change is the format of the SSPP template. EDE used a Microsoft Word format whereas ARC-AMPE is an Excel spreadsheet.

Control mapping

The mapping of the controls found in the EDE audit baseline (based on NIST SP 800-53 Revision 4) to their new locations in ARC-AMPE (based on NIST SP 800-53 Revision 5) are included in the table below. The table lists the EDE control directly compared with the ARC-AMPE equivalent control name, as applicable. The table also documents any new ARC-AMPE controls that do not have EDE equivalents, as well as those controls that have been combined or withdrawn for ARC-AMPE.

Note also that all references to NIST SP 800-53 Revision 5 included below are based on version 5.1.1, which was issued on November 7, 2023.

Maintenance (MA)

The set of controls in this family focus on how the Exchange shall: (1) perform periodic and timely maintenance on organizational information systems; and (2) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

EDE		ARC-AMPE	
Control	**System Maintenance Policy and Procedures**	**Control**	**Policy and Procedures**
MA-1: System Maintenance Policy and Procedures The organization: **a.** Develops, documents, and disseminates to applicable personnel: **1.** A system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and **2.** Procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls. **b.** Reviews and updates (as necessary) the current: **1.** System maintenance policy within every three (3) years; and **2.** System maintenance procedures within every three (3) years. **c.** System maintenance policy and procedures must ensure that contractors having access to records (i.e., files or data) maintained in a system of records are contractually bound to be covered by the Privacy Act.		**MA-01: Policy and Procedures** **a.** Develop, document, and disseminate to applicable personnel or roles: **1.** Organization-level maintenance policy that: **(a)** Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and **(b)** Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines; and **2.** Procedures to facilitate the implementation of the maintenance policy and the associated maintenance controls; **b.** Designate an organization-defined official to manage the development, documentation, and dissemination of the maintenance policy and procedures; and **c.** Review and update the current maintenance: **1.** Policy at least every one (1) year and following organization-defined events; and **2.** Procedures at least every one (1) year and following organization-defined events.	
Control	**Controlled Maintenance**	**Control**	**Controlled Maintenance**
MA-2: Controlled Maintenance The organization: **a.** Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements; **b.** Approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location; **c.** Requires that the applicable business owner (or an official designated in the applicable security plan) explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs; **d.** Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs; **e.** Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions; and **f.** Includes organization-defined maintenance-related information (defined in the applicable security plan) in organizational maintenance records.		**MA-02: Controlled Maintenance** **a.** Schedule, document, and review records of maintenance, repair, and replacement on system components in accordance with manufacturer or vendor specifications and/or organizational requirements; **b.** Approve and monitor all maintenance activities, whether performed on site or remotely and whether the system or system components are serviced on site or removed to another location; **c.** Require that organization-defined personnel or roles explicitly approve the removal of the system or system components from organizational facilities for off-site maintenance, repair, or replacement; **d.** Sanitize equipment to remove the following information from associated media prior to removal from organizational facilities for off-site maintenance, repair, or replacement: all organizational information; **e.** Check all potentially impacted controls to verify that the controls are still functioning properly following maintenance, repair, or replacement actions; and **f.** Include the following information in organizational maintenance records: maintenance-related information.	

EDE		ARC-AMPE	
Control	**Maintenance Tools**	**Control**	**Maintenance Tools**
MA-3: Maintenance Tools The organization approves, controls, and monitors information system maintenance tools.		**MA-03: Maintenance Tools** **a.** Approve, control, and monitor the use of system maintenance tools; and **b.** Review previously approved system maintenance tools at least every one (1) year.	
Control	**Inspect Tools**	**Control**	**Inspect Tools**
MA-3 (1): Inspect Tools The organization inspects the maintenance tools carried into a facility by maintenance personnel for any improper or unauthorized modifications.		**MA-03(01): Inspect Tools** Inspect the maintenance tools used by maintenance personnel for improper or unauthorized modifications.	
Control	**Inspect Media**	**Control**	**Inspect Media**
MA-3 (2): Inspect Media The organization checks media containing diagnostic and test programs for malicious code before the media are used in the information system.		**MA-03(02): Inspect Media** Check media containing diagnostic and test programs for malicious code before the media are used in the system.	
Control	**Prevent Unauthorized Removal**	**Control**	**Prevent Unauthorized Removal**
MA-3 (3): Prevent Unauthorized Removal The organization prevents the unauthorized removal of maintenance equipment containing organizational information by: **c.** Verifying that there is no organizational or sensitive information contained on the equipment; **a.** Sanitizing or destroying the equipment; **b.** Retaining the equipment within the facility; or **c.** Obtaining an exemption, in writing, from the CIO or his/her designated representative explicitly authorizing removal of the equipment from the facility.		**MA-03(03): Prevent Unauthorized Removal** Prevent the removal of maintenance equipment containing organizational information by: **a.** Verifying that there is no organizational information contained on the equipment; **b.** Sanitizing or destroying the equipment; **c.** Retaining the equipment within the facility; or **d.** Obtaining an exemption from organization-defined personnel or roles explicitly authorizing removal of the equipment from the facility.	
Control	**N/A**	**Control**	**Execution with Privilege**
New NIST SP 800-53 Rev. 5 Control and applicable to ARC-AMPE		**MA-03(05): Execution with Privilege** Monitor the use of maintenance tools that execute with increased privilege.	
Control	**N/A**	**Control**	**Software Updates and Patches**
New NIST SP 800-53 Rev. 5 Control and applicable to ARC-AMPE		**MA-03(06): Software Updates and Patches** Inspect maintenance tools to ensure the latest software updates and patches are installed.	
Control	**Nonlocal Maintenance**	**Control**	**Nonlocal Maintenance**
MA-4: Nonlocal Maintenance The organization monitors and controls nonlocal maintenance and diagnostic activities; and prohibits nonlocal system maintenance unless explicitly authorized, in writing, by the CIO		**MA-04: Nonlocal Maintenance** **a.** Approve and monitor nonlocal maintenance and diagnostic activities; **b.** Allow the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the system;	

EDE	ARC-AMPE
or his/her designated representative. If nonlocal maintenance and diagnostic actives are authorized, the organization: **a.** Allows the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system; **b.** Employs strong identification and authentication techniques in the establishment of nonlocal maintenance and diagnostic sessions; **c.** Maintains records for nonlocal maintenance and diagnostic activities; and **d.** Terminates all sessions and network connections when nonlocal maintenance is completed. **Implementation Standards** **1.** If password-based authentication is used during remote maintenance, change the passwords following each remote maintenance service. **2.** Media used during remote maintenance must be sanitized in accordance with NIST SP 800-88, as amended.	**c.** Employ strong authentication in the establishment of nonlocal maintenance and diagnostic sessions; **d.** Maintain records for nonlocal maintenance and diagnostic activities; and **e.** Terminate session and network connections when nonlocal maintenance is completed.
Control — **Auditing and Review**	**Control** — **Logging and Review**
MA-4 (1): Auditing and Review The organization: **a.** Audits nonlocal maintenance and diagnostic sessions using available audit events; and **b.** Reviews the records of the maintenance and diagnostic sessions.	**MA-04(01): Logging and Review** **a.** Log organization-defined audit events, as defined in the organization's formal audit policy, for nonlocal maintenance and diagnostic sessions; and **b.** Review the audit records of the maintenance and diagnostic sessions to detect anomalous behavior.
Control — **Document Nonlocal Maintenance**	**Control** — **N/A**
MA-4 (2): Document Nonlocal Maintenance The organization documents in the information system's security plan the policies and procedures for the establishment and use of nonlocal maintenance and diagnostic connections.	**Withdrawn Control**: Incorporated into **MA-01** and **MA-04**.
Control — **Maintenance Personnel**	**Control** — **Maintenance Personnel**
MA-5: Maintenance Personnel The organization: **a.** Establishes a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel; **b.** Ensures that non-escorted personnel performing maintenance on the information system have required access authorizations; and **c.** Designates organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.	**MA-05: Maintenance Personnel** **a.** Establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel; **b.** Verify that non-escorted personnel performing maintenance on the system possess the required access authorizations; and **c.** Designate organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

EDE		ARC-AMPE	
Control	**Timely Maintenance**	**Control**	**Timely Maintenance**
MA-06: Timely Maintenance The organization obtains maintenance support and/or spare parts for defined key information system components (defined in the applicable security plan) within the applicable Recovery Time Objective (RTO) specified in the contingency plan. **Implementation Standard** The organization defines a list of security-critical information system components and/or key information technology components.		**MA-06: Timely Maintenance** Obtain maintenance support and/or spare parts for organization-defined information system component within the applicable Recovery Time Objective (RTO) (specified in the system Contingency Plan) of failure.	

References

NIST SP 800-53 Revision 5.1.1

NIST SP 800-53 Revision 4

CMS Standards

Legal disclaimer

This white paper is provided by Coalfire Systems, Inc. or its subsidiaries (“Coalfire”) for informational purposes only. This white paper is the property of Coalfire and is protected by U.S. and international copyright laws. Unauthorized use, reproduction, or distribution of this white paper, in whole or in part, is strictly prohibited. Factual information included in this white paper has been taken from sources that Coalfire believes to be reliable, but its accuracy, completeness, or interpretation cannot be guaranteed. Information is current as of the date of this white paper only and is subject to change without notice. This white paper is provided “as-is” with no warranties, including any warranty of merchantability, fitness for a particular purpose, and non-infringement. Coalfire expressly disclaims all liability arising from or relating to the use of any information or material included in this white paper for any purpose, including any actions taken or not taken based on the contents of this white paper. You are solely responsible for making your own independent assessment of the information in this white paper and for the development, implementation, and execution of your information security program. For questions regarding any legal or compliance matters referenced in this white paper, you should consult your legal counsel, security advisor, or the relevant standard authority.

About the authors

Jessica Payne, Consultant

Jessica joined Coalfire in 2024 with five prior years of cybersecurity consulting experience. She supports our clients as a Consultant for the GRC Healthcare team where she specializes in cybersecurity risk management, cybersecurity program advisory, and compliance for the healthcare industry.

Her extensive experience in cybersecurity consulting allows her to provide customized solutions and guidance on industry best practices, greatly improving client security postures and ensuring compliance with regulatory standards. She is dedicated to ongoing improvement and to staying abreast of the latest cybersecurity trends and technologies to offer innovative solutions to her clients.

Ian Walters, Principal

Ian is a seasoned cybersecurity professional with a wealth of experience across a spectrum of frameworks and standards, including NIST SP 800-53, HIPAA, ISO 27001, ISO 20000, and ISO 9001.

With a meticulous eye for detail and a strategic mindset, Ian excels in developing tailored solutions to ensure compliance and mitigate risks within complex organizational environments. His expertise extends to leading audits and risk assessments, as well as providing advisory for driving continuous improvement initiatives to enhance cybersecurity posture and operational resilience.

About Coalfire

The world's leading technology infrastructure providers, SaaS companies, and enterprises – including the top 5 cloud service providers and 8 of the top 10 SaaS businesses – rely on Coalfire to strengthen their security posture and secure their digital transformations. As the largest firm dedicated to cybersecurity, Coalfire delivers a comprehensive suite of advisory and managed services, spanning cyber strategy and risk, cloud security, threat and vulnerability management, application security, privacy, and compliance management. A proven leader in cybersecurity for the past 20 years, Coalfire combines extensive cloud expertise, advanced technology, and innovative approaches that fuel success. For more information, visit **Coalfire.com**.

WP_ACA CMS Controls Migration (Maintenance (MA))_07142025