COALFIRE

WHITE PAPER

# Migration from EDE to ARC-AMPE Media Protection (MP) controls

## CMS requirements for Direct Enrollment Entities

JESSICA PAYNE, CONSULTANT
IAN WALTERS, PRINCIPAL

877-224-8077 | info@coalfire.com | Coalfire.com

# Table of contents

**Purpose** ..... **2**
**Background** ..... **3**
Affordable Care Act ..... 3
Enhanced Direct Enrollment ..... 3
CMS oversight ..... 3
ARC-AMPE ..... 4
**Control mapping** ..... **4**
Media Protection (MP) ..... 5
**References** ..... **9**
**Legal disclaimer** ..... **10**

# 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 Media Protection 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 | 12 |
| **Media Protection (This Document)** | **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.

# Media Protection (MP)

The set of controls in this family focus on how the Exchange shall: (1) protect IT system media, both paper and digital; (2) limit access to information on IT system media to authorized users; and (3) sanitize or destroy IT system media before disposal or release for reuse.

| EDE | | ARC-AMPE | |
|---|---|---|---|
| **Control** | **Media Protection Policy and Procedures** | **Control** | **Policy and Procedures** |
| **MP-1: Media Protection Policy and Procedures**<br>The organization:<br>**a.** Develops, documents, and disseminates to applicable personnel:<br>**1.** A media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and<br>**2.** Procedures to facilitate the implementation of the media protection policy and associated media protection controls.<br>**b.** Reviews and updates (as necessary) the current:<br>**1.** Media protection policy within every three (3) years; and<br>**2.** Media protection procedures within every three (3) years.<br>*"Applicable personnel," as referred to in MP-1(a), includes employees and contractors with potential access to personally identifiable information (PII).* | | **MP-01: Policy and Procedures**<br>**a.** Develop, document, and disseminate to applicable personnel or roles:<br>**1.** Organization-level media protection policy that:<br>**(a)** Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and<br>**(b)** Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and<br>**2.** Procedures to facilitate the implementation of the media protection policy and the associated media protection controls;<br>**b.** Designate organization-defined officials to manage the development, documentation, and dissemination of the media protection policy and procedures; and<br>**c.** Review and update the current media protection:<br>**1.** Policy at least every one (1) year and following organization-defined events; and<br>**2.** Procedures at least every one (1) year and following organization-defined events. | |

| EDE | | ARC-AMPE | |
|---|---|---|---|
| **Control** | **Media Access** | **Control** | **Media Access** |
| **MP-2: Media Access**<br>The organization restricts access to sensitive information, such as Personally Identifiable Information (PII), residing on digital and non-digital media to authorized individuals using automated mechanisms to control access to media storage areas in compliance with the latest revision of NIST SP 800-88, Guidelines for Media Sanitization, to defined personnel or roles (defined personnel or roles must be authorized individuals with a valid need to know as defined in the applicable security plan) by disabling:<br>**a.** CD/DVD writers and allowing access to using CD/DVD viewing and downloading capabilities only to persons specified or in defined roles; and<br>**b.** USB ports and allowing access to using USB device capabilities only to persons specified or in defined roles.<br><br>**Implementation Standards**<br>**1.** The organization defines types of digital (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, and digital video disks) and non-digital media (e.g., paper, microfilm) and non-digital media.<br>**2.** Define a list of individuals with authorized access to defined media types.<br>**3.** Define the types of security measures to be used in protecting defined media types. | | **MP-02: Media Access**<br>Restrict access to all types of digital and non-digital media to organization-defined personnel or roles. | |
| **Control** | **Media Marking** | **Control** | **Media Marking** |
| **MP-3: Media Marking**<br>The organization:<br>**a.** Marks information system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and<br>**b.** Does not exempt any removable media types from marking. | | **MP-03: Media Marking**<br>**a.** Marks information system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and<br>**b.** Exempt specific types of media or hardware components, as specified, in writing, by the Chief Information Officer (CIO) or their designated representative, from marking if the media remains within a secure environment. | |
| **Control** | **Media Storage** | **Control** | **Media Storage** |
| **MP-4: Media Storage**<br>The organization:<br>**a.** Physically controls and securely stores all magnetic tapes, external/removable hard drives, flash/thumb drives, diskettes, compact disks, and digital video disks within organization-defined controlled areas; encrypts digital media via a FIPS 140-2 compliant encryption module; and for non-digital media, provides secure storage in locked cabinets or safes.<br>**b.** Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures. | | **MP-04: Media Storage**<br>**a.** Physically control and securely store digital and/or non-digital media: all magnetic tapes, external removable hard drives, flash/thumb drives, diskettes, compact disks, and digital video disks. Securely store digital and non-digital media within organization-defined controlled areas; and<br>**b.** Protect system media types defined in MP-4a until the media are destroyed or sanitized using approved equipment, techniques, and procedures. | |

| EDE | | ARC-AMPE | |
|---|---|---|---|
| **Implementation Standard**<br>**1.** If PII is recorded on magnetic media with other data, the media should be protected as if all the data contained consisted of personally identifiable information.<br>**2.** Define controlled areas within facilities where the information and information system reside. | | | |
| **Control** | **Media Transport** | **Control** | **Media Transport** |
| **MP-5: Media Transport**<br>The organization:<br>**a.** Protects and controls digital and non-digital media defined within the latest revision of NIST SP 800-88, Guidelines for Media Sanitization containing sensitive information during transport outside of controlled areas using cryptography and tamper evident packaging, and;<br>**1.** If hand carried, using securable container (e.g., locked briefcase) via authorized personnel, or<br>**2.** If shipped, trackable with receipt by commercial carrier.<br>**b.** Maintains accountability for information system media during transport outside of controlled areas;<br>**c.** Documents activities associated with the transport of information system media; and<br>**d.** Restricts the activities associated with the transport of information system media to authorized personnel.<br>**e.** Protects and controls digital media that contains personally identifiable information (PII) during transport outside of controlled areas using FIPS 140-2 validated encryption.<br><br>**Implementation Standard**<br>**1.** Protect and control non-digital PII media during transport outside of controlled areas and restricts the activities associated with transport of such media to authorized personnel. Non-digital PII must be in locked cabinets or sealed packing cartons while in transit.<br>**2.** The organization protects and controls magnetic tapes, external/removable hard drives, flash/thumb drives, diskettes, compact disks, and digital video disks during transport outside of controlled areas, and encrypts digital media via a FIPS 140-2 compliant encryption module.<br>**3.** Define security measures to protect digital and non-digital media in transport. | | **MP-05: Media Transport**<br>**a.** Protect and control digital and non-digital media containing sensitive information, such as Personally Identifiable Information (PII), during transport outside of controlled areas using organization-defined controls such as:<br>• Most current FIPS 140-compliant encryption module;<br>• Locked/securable containers or tamper-evident packaging transported via authorized personnel;<br>• A trackable receipt by the commercial shipping carrier; and<br>• Sealed packing cartons for non-digital media containing sensitive information.<br>**b.** Maintain accountability for system media during transport outside of controlled areas;<br>**c.** Document activities associated with the transport of system media; and<br>**d.** Restrict the activities associated with the transport of system media to authorized personnel. | |
| **Control** | **Cryptographic Protection** | **Control** | **N/A** |
| **MP-5 (4): Cryptographic Protection**<br>The information system implements cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas. | | Withdrawn control: Incorporated into **SC-28(01)** | |
| **Control** | **Media Sanitization** | **Control** | **Media Sanitization** |
| **MP-6: Media Sanitization**<br>The organization: | | **MP-06: Media Sanitization**<br>**a.** Sanitize digital and non-digital system media prior to disposal, release out of organizational control, or release | |

<table>
<tr><th colspan="2">EDE</th><th colspan="2">ARC-AMPE</th></tr>
<tr><td colspan="2">a. Sanitizes both digital and non-digital information system media prior to disposal, release out of organizational control, or release for reuse using defined sanitization techniques and procedures (defined in the applicable security plan in accordance with the latest revision of NIST SP 800-88, Guidelines for Media Sanitization; and<br>b. Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.<br><br>Implementation Standard<br>1. Finely shred, using a minimum of cross-cut shredding, hard-copy documents, using approved equipment, techniques, and procedures.<br>2. Surplus equipment is stored securely while not in use, and disposed of or sanitized in accordance with NIST 800-88 when no longer required.<br>3. Support the capability to sanitize disk space when released from an instance (container) image file.</td><td colspan="2">for reuse using defined sanitization techniques and procedures in accordance with the most current NIST SP 800-88 guidelines; and<br>b. Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.</td></tr>
<tr><td>Control</td><td>N/A</td><td>Control</td><td>Review, Approve, Track, Document, and Verify</td></tr>
<tr><td colspan="2"></td><td colspan="2">MP-06(01): Review, Approve, Track, Document, and Verify<br>Review, approve, track, document, and verify media sanitization and disposal actions.</td></tr>
<tr><td>Control</td><td>Media Use</td><td>Control</td><td>Media Use</td></tr>
<tr><td colspan="2">MP-7: Media Use<br>The organization:<br>a. Prohibits the use of personally owned media on organizational information systems or system components using defined security safeguards (defined in the applicable security plan).<br>b. Restricts the use of portable storage and mobile devices on information systems and networks containing PII, without using device ownership, media sanitization and encryption controls.</td><td colspan="2">MP-07: Media Use<br>a. Prohibit the use of personally owned media (e.g., flash drives, external hard disk drives, and other portable storage and media devices) on organization-defined systems and networks using organization-defined security safeguards; and<br>b. Prohibit the use of portable storage devices in organizational systems when such devices have no identifiable owner.</td></tr>
<tr><td>Control</td><td>Prohibit Use Without Owner</td><td>Control</td><td>N/A</td></tr>
<tr><td colspan="2">MP-7 (1): Prohibit Use Without Owner<br>The organization prohibits the use of portable storage devices in organizational information systems when such devices have no identifiable owner.</td><td colspan="2">Withdrawn control: Incorporated into MP-07.</td></tr>
</table>

# 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 (Media Protection (MP))_07142025