COALFIRE

WHITE PAPER

Migration from EDE to ARC-AMPE Assessment, Authorization, and Monitoring (CA) 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

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 Assessment, Authorization, and Monitoring 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 (This document)	**12**
Configuration Management	25
Contingency Planning	16
Identification and Authentication	21
Incident Response	15
Maintenance	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.

Assessment, Authorization, and Monitoring (CA)

The set of controls in this family focus on how the Exchange shall: (1) periodically assess the security controls in Exchange IT systems to determine if the controls are effective in their application; (2) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in Exchange IT systems; (3) authorize the operation of Exchange IT systems and any associated IT system connections; and (4) monitor IT system security controls on an ongoing basis to ensure the continued effectiveness of the controls

EDE		ARC-AMPE	
Control	**Security Assessment and Authorization Policies and Procedures**	**Control**	**Policies and Procedures**
CA-1: Security Assessment and Authorization Policies and Procedures The organization: **a.** Develops, documents, and disseminates to applicable personnel: **1.** A security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and **2.** Procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls; and **b.** Reviews and updates (as necessary) the current: **1.** Security assessment and authorization policy at least every three (3) years; and **2.** Security assessment and authorization procedures at least every three (3) years.		**CA-01: Policies and Procedures** **a.** Develop, document, and disseminate to organization-defined personnel and roles: **1.** Organization-level assessment, authorization, and monitoring 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 assessment, authorization, and monitoring policy and the associated assessment, authorization, and monitoring controls; **b.** Designate an organization-defined official to manage the development, documentation, and dissemination of the assessment, authorization, and monitoring policy and procedures; and **c.** Review and update the current assessment, authorization, and monitoring: **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	**Security Assessments**	**Control**	**Control Assessments**
CA-2: Security Assessments The organization: **a.** Develops a security and privacy assessment plan that describes the scope of the assessment including: **1.** Security and privacy controls and control enhancements under assessment; **2.** Assessment procedures to be used to determine control effectiveness; and **3.** Assessment environment, assessment team, and assessment roles and responsibilities; **b.** Assesses the security and privacy controls in the information system and its environment of operation every three hundred sixty-five (365) days to determine the extent to which the controls are implemented correctly, operating as intended, and producing the		**CA-02: Control Assessments** **a.** Select the appropriate assessor or assessment team for the type of assessment to be conducted; **b.** Develop a control assessment plan that describes the scope of the assessment, including: **1.** Controls and control enhancements under assessment; **2.** Assessment procedures to be used to determine control effectiveness; and **3.** Assessment environment, assessment team, and assessment roles and responsibilities; **c.** Ensure the control assessment plan is reviewed and approved by the Authorizing Official or designated representative prior to conducting the assessment; **d.** Assess the controls in the system and its environment of operation as specified in the supplemental control requirements & guidance to determine the extent to	

<table>
<tr><th>EDE</th><th>ARC-AMPE</th></tr>
<tr><td>desired outcome with respect to meeting established security requirements;
c. Produces an assessment report that documents the results of the assessment; and
d. Provides the results of the security and privacy control assessment within thirty (30) days after its completion, in writing, to the organizational official who is responsible for reviewing the assessment documentation and updating system security documentation where necessary to reflect any changes to the system.

Implementation Standards
1. An independent assessment of all security and privacy controls must be conducted before the organization’s Authorizing Official issues the authority to operate for all newly implemented, or significantly changed, systems.
2. Information system security and privacy assessments should be conducted annually. These assessments can be conducted by independent assessors or by the performance of self-assessments against the information system.
3. The annual security and privacy assessment requirement requires all security and privacy controls attributable to a system to be assessed.</td><td>which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements;
e. Produce a control assessment report that documents the results of the assessment; and
f. Provide the results of the control assessment to the Business Owner responsible for the system and personnel responsible for reviewing the assessment documentation, and updating security and privacy documentation where necessary to reflect any changes to the system within thirty (30) days after its completion in writing.</td></tr>
<tr><td>Control | Independent Assessors</td><td>Control | Independent Assessors</td></tr>
<tr><td>CA-2 (1): Independent Assessors
The organization employs assessors or assessment teams with NIST-defined level of independence to conduct security and privacy control assessments of the organization’s information system.</td><td>CA-02(01): Independent Assessors
Employ independent assessors or assessment teams to conduct control assessments.</td></tr>
<tr><td>Control | System Interconnections</td><td>Control | Information Exchange</td></tr>
<tr><td>CA-3: System Interconnections
The organization:
a. Authorizes connections from the organization’s information system to other information systems through the use of interconnection security agreements (ISA);
b. Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and
c. Reviews and updates the interconnection agreements on an ongoing basis to verify enforcement of security requirements; and;
d. Establishes system-to-system connections with CMS through the CMS ISA process.
e. Only activates a system interconnection (including testing) when a signed ISA is in place.
Implementation Standards</td><td>CA-03: Information Exchange
a. Approve and manage the exchange of information between the system and other systems using interconnection security agreements (ISA), information exchange security agreements, memoranda of understanding or agreement (MOU/MOA), service level agreements (SLA), user agreements, nondisclosure agreements (NDA), or other exchange agreements;
b. Document, as part of each exchange agreement, the interface characteristics, security and privacy requirements, controls, and responsibilities for each system, and the impact level of the information communicated; and
c. Review and update the agreements at least every one (1) year.</td></tr>
</table>

EDE		ARC-AMPE	
1. Record each system interconnection in the security plan for the system that is connected to the remote location. 2. The ISA is updated following significant changes to the system, organization, or the nature of the electronic sharing of information that could impact the validity of the agreement. 3. The ISA must be fully signed and executed prior to any interconnection outside of the system boundary taking place for any purpose (within the constraints of the control).			
Control	**Restrictions on External System Connections**	**Control**	**N/A**
CA-3 (5): Restrictions on External System Connections The organization employs, and documents, in the applicable security plan a “deny all, permit-by-exception” policy for allowing defined information systems that receive, process, store, or transmit Personally Identifiable Information (PII) to connect to external information systems.		**Withdrawn Control**: Moved to **SC-7(5)**.	
Control	**Plan of Action and Milestones**	**Control**	**Plan of Action and Milestones**
CA-5: Plan of Action and Milestones The organization: a. Develops a plan of action and milestones (POA&M) for the information system within thirty (30) days of the final results for every internal/external audit/review or test (e.g., security controls assessment, penetration test) to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; b. Updates the existing POA&M monthly until all the findings are resolved based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities. **Implementation Standard** Remediates vulnerabilities rated as Critical severity within fifteen (15) calendar days, High severity within thirty (30) calendar days, Moderate severity within ninety (90) calendar days and Low severity within three hundred and sixty-five (365) calendar days.		**CA-05: Plan of Action and Milestones** **a.** Develop a plan of action and milestones (POA&M) for the system to document the planned remediation actions of the organization to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system; and **b.** Update existing POA&M in accordance with the frequency documented in the organization's Information Security Continuous Monitoring (ISCM) strategy based on the findings from control assessments, independent audits or reviews, and continuous monitoring activities.	
Control	**Security Authorization**	**Control**	**Authorization**
CA-6: Security Authorization The organization: **a.** Ensures that the organizational authorizing official authorizes the information system for processing before commencing operations; and **b.** Updates the security authorization: **1.** Within every three (3) years;		**CA-06: Authorization** **a.** Assign a senior official as the Authorizing Official (AO) for the system; **b.** Assign a senior official as the AO for common controls available for inheritance by organizational systems; **c.** Ensure that, before commencing operations, the AO for the system:	

EDE	ARC-AMPE
2. When significant changes are made to the system; 3. When changes in requirements result in the need to process data of a higher sensitivity; 4. When changes occur to authorizing legislation or federal requirements; 5. After the occurrence of a serious security violation which raises questions about the validity of an earlier security authorization; and 6. Prior to expiration of a previous security authorization. **c.** If the organization maintains a system-to-system connection with CMS through an executed ISA, the CMS-granted request to connect is updated: 1. Every year or three hundred sixty-five days; 2. When significant changes are made to the system; 3. When changes in requirements result in the need to process data of a higher sensitivity; 4. When changes occur to authorizing legislation or federal requirements; 5. After the occurrence of a serious security violation which raises questions about the validity of an earlier security authorization; and 6. Prior to expiration of a previous security authorization.	1. Accepts the use of common controls inherited by the system; and 2. Authorizes the system to operate; **d.** Ensure that the AO for common controls authorizes the use of those controls for inheritance by organizational systems; and **e.** Update the authorizations consistent with the frequency identified in the supplemental control requirements and guidance.
Control **Continuous Monitoring**	**Control** **Continuous Monitoring**
CA-7: Continuous Monitoring The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes: **a.** Establishment of organizationally defined metrics (defined in the applicable security plan) to be monitored annually and in accordance with the basic requirements set forth in the Non-Exchange Entity Information Security and Privacy Continuous Monitoring Strategy Guide consistent with the NIST SP 800-137, and **b.** Establishment of defined frequencies (defined in the applicable security plan) for monitoring and defined frequencies (defined in the applicable security plan) for assessments supporting such monitoring; **c.** Ongoing security control assessments in accordance with the organizational continuous monitoring strategy; **d.** Ongoing security status monitoring of organizationally defined metrics in accordance with the organizational continuous monitoring strategy; **e.** Correlation and analysis of security-related information generated by assessments and monitoring; **f.** Response actions to address results of the analysis of security-related information;	**CA-07: Continuous Monitoring** Develop a system-level continuous monitoring strategy and implement continuous monitoring in accordance with the organization-level continuous monitoring strategy that includes: **a.** Establishing the following system-level metrics to be monitored based on the organization security and privacy goals and in accordance with organization's Information Security Continuous Monitoring (ISCM) strategy; **b.** Establishing at least once a month scans for operating system, databases, and web applications for monitoring and no less than at least every one (1) year for assessment of control effectiveness; **c.** Ongoing control assessments in accordance with the continuous monitoring strategy; **d.** Ongoing monitoring of system and organization-defined metrics in accordance with the continuous monitoring strategy; **e.** Correlation and analysis of information generated by control assessments and monitoring; **f.** Response actions to address results of the analysis of control assessment and monitoring information; and **g.** Reporting the security and privacy status of the system to organization-defined personnel or roles consistent with the frequency in the applicable System Security and Privacy Plan (SSPP) but no less than at least every thirty (30) days (monthly).

EDE		ARC-AMPE	
g. Reporting the security status of organization and the information system to defined personnel or roles (defined in the applicable security plan) monthly; and **h.** Reporting the security status of organizational systems to defined personnel or roles (defined in the applicable security plan) at organizational-defined frequency, and reporting to CMS as specified in the implementation standard. **Implementation Standards** **1.** When subject to a legal investigation (e.g., of an insider threat), continuous monitoring records must be maintained until released by the investigating authority. **2.** Monitor systems, appliances, devices, and applications (including databases). **3.** Identify specific review requirements for the following: **a.** Plan of Action and Milestones (POA&M) **b.** Reporting of significant changes to the organizational information system environment			
Control	**Independent Assessment**	**Control**	**Independent Assessment**
CA-7 (1): Independent Assessment The organization employs assessors or assessment teams with a defined level of independence to monitor the security and privacy controls in the information system on an ongoing basis. **Implementation Standard** Implementation of independent security and privacy assessment and the Security Assessment Report (SAR) follows CMS specifications.		**CA-07(01): Independent Assessment** Employ independent assessors or assessment teams to monitor the controls in the system on an ongoing basis.	
Control	**N/A**	**Control**	**Risk Monitoring**
New NIST SP 800-53 Rev.5 Control and applicable to ARC-AMPE		**CA-07(04): Risk Monitoring** Ensure risk monitoring is an integral part of the continuous monitoring strategy that includes the following: **a.** Effectiveness monitoring; **b.** Compliance monitoring; and **c.** Change monitoring.	
Control	**Penetration Testing**	**Control**	**Penetration Testing**
CA-8: Penetration Testing The organization conducts both internal and external penetration testing, within every three hundred sixty-five (365) days, on defined information systems or system components (defined in the applicable system security plan), or whenever there has been a significant change to the system. At a minimum, penetration testing must be conducted to determine: **a.** How well the system tolerates real world-style attack patterns; **b.** The likely level of sophistication an attacker needs to successfully compromise the system; **c.** Additional countermeasures that could mitigate threats against the system; and		**CA-08: Penetration Testing** Conduct penetration testing at least every one (1) year on organization-defined systems or system components as agreed with the penetration testers in the Rules of Engagement.	

EDE		ARC-AMPE	
d. Defenders' ability to detect attacks and respond appropriately. **Implementation Standards** **1.** Conduct internal and external penetration testing as needed but no less often than once every three hundred sixty-five (365) days. **2.** Penetration tests are performed when new risks and threats potentially affecting the system/applications are identified and reported or upon request from CMS. **3.** Penetration testing on a production system must be conducted in a manner that minimized risk of information corruption or service outage.			
Control	**Independent Penetration Agent or Team**	**Control**	**Independent Penetration Testing Agent or Team**
CA-8 (1): Independent Penetration Agent or Team The organization employs an independent penetration agent or penetration team to perform penetration testing on the information system or system components. **Implementation Standard** The independent penetration agent or penetration team must be the organization CISO approved independent penetration test vendor.		**CA-08(01): Independent Penetration Testing Agent or Team** Employ an independent penetration testing agent or team to perform penetration testing on the system or system components.	
Control	**Internal System Connections**	**Control**	**Internal System Connections**
CA-9: Internal System Connections The organization: **a.** Authorizes connections of defined internal information system components or classes of components (defined in the applicable security plan) to the information system; and **b.** Documents, for each internal connection, the interface characteristics, security and privacy requirements, and the nature of the information communicated. Documentation must also address authorization and responsibilities of the receiving information system for protecting any PII. **Implementation Standard** The security plan will identify the types of personally owned equipment that may be internally connected with organizational information systems and networks.		**CA-09: Internal System Connections** **a.** Authorize internal connections of organization-defined system components or classes of components to the system; **b.** Document, for each internal connection, the interface characteristics, security and privacy requirements, and the nature of the information communicated; **c.** Terminate internal system connections after issuance of an order by the organization's Chief Information Officer (CIO), Chief Information Security Officer (CISO), or senior privacy official and when such internal system connections no longer support the organization's missions or business functions; and **d.** Review at least every one (1) year the continued need for each internal connection.	

References

NIST SP 800-53 Revision 5.1.1

NIST SP 800-53 Revision 4

CMS Standards

Legal disclaimer

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 (Authorization, and Monitoring (CA)) _07142025