COALFIRE

WHITE PAPER

Migration from EDE to ARC-AMPE Risk Assessment (RA) 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 Risk Assessment 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	8
Physical and Environmental Protection	9
Planning	6
Program Management	5
Personnel Security	8
Personally Identifiable Information Processing and Transparency	10
Risk Assessment (This Document)	**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.

Risk Assessment (RA)

The set of controls in this family focus on how the Exchange shall periodically assess the risk to Exchange operations (including mission, functions, image, or reputation), Exchange assets, and individuals, resulting from the operation of Exchange IT systems and the associated processing, storage, or transmission of Exchange information.

EDE		ARC-AMPE	
Control	**Risk Assessment Policy and Procedure**	**Control**	**Policy and Procedures**
RA-1: Risk Assessment Policy and Procedure The organization: **a.** Develops, documents, and disseminates to applicable personnel: **1.** A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and **2.** Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls on information systems and paper records; and **b.** Reviews and updates (as necessary) the current: **1.** Risk assessment policy within every three (3) years; and **2.** Risk assessment procedures within every three (3) years.		**RA-01: Policy and Procedures** **a.** Develop, document, and disseminate to organization-defined personnel or roles: **1.** Organization-level risk assessment 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 risk assessment policy and the associated risk assessment controls; **b.** Designate an organization-defined official to manage the development, documentation, and dissemination of the risk assessment policy and procedures; and **c.** Review and update the current risk assessment: **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	**Risk Assessment**	**Control**	**Security Categorization**
Existing NIST SP 800-53 Rev.4 control and new to ARC-AMPE.		**RA-02: Security Categorization** **a.** Categorize the system and information it processes, stores, and transmits; **b.** Document the security categorization results, including supporting rationale, in the security plan for the system; and **c.** Verify that the Authorizing Official (AO) or AO's designated representative reviews and approves the security categorization decision.	
Control	**Risk Assessment**	**Control**	**Risk Assessment**
RA-3: Security Categorization The organization: **a.** Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits; **b.** Documents risk assessment results in the applicable security plan;		**RA-03: Risk Assessment** **a.** Conduct a risk assessment, including: **1.** Identifying threats to and vulnerabilities in the system; **2.** Determining the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system; the information it processes, stores, or transmits; and any related information; and	

<table>
<tr><th colspan="2">EDE</th><th colspan="2">ARC-AMPE</th></tr>
<tr><td colspan="2">c. Reviews risk assessment results within every three hundred sixty-five (365) days;
d. Disseminates risk assessment results to affected stakeholders and Business Owners(s); and
e. Updates the risk assessment every three (3) years or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security or authorization state of the system.
<b>Implementation Standard</b>
The organization conducts an information security risk assessment and documents risk assessment results.</td><td colspan="2">3. Determining the likelihood and impact of adverse effects on individuals arising from the processing of Personally Identifiable Information (PII);
b. Integrate risk assessment results and risk management decisions from the organization and mission or business process perspectives with system-level risk assessments;
c. Document risk assessment results in security and privacy plans, risk assessment report, and any additional organization-defined documents;
d. Review risk assessment results at least every one (1) year or when a significant change occurs
e. Disseminate risk assessment results to organization-defined personnel or roles; and
f. Update the risk assessment at least every three (3) years at a minimum or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security or privacy state of the system.</td></tr>
<tr><td><b>Control</b></td><td><b>Vulnerability Scanning</b></td><td><b>Control</b></td><td><b>Vulnerability Monitoring and Scanning</b></td></tr>
<tr><td colspan="2"><b>RA-5: Vulnerability Scanning</b>
a. Scans for vulnerabilities in the information system and hosted applications, operating system, web application, and database scans (as applicable) within every thirty (30) days and when new critical or high vulnerabilities potentially affecting the system/applications are identified and reported no less than 72 hours;
b. Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
1. Enumerating platforms, software flaws, and improper configurations;
2. Formatting checklists and test procedures;
3. Measuring vulnerability impact;
c. Analyzes vulnerability scan reports and results from security control assessments;
d. Remediates legitimate vulnerabilities based on the Business Owner’s risk prioritization in accordance with an organizational assessment of risk; and
e. Shares information obtained from the vulnerability scanning process and security control assessments with affected/related stakeholders on a “need to know” basis to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).
<b>Implementation Standards</b>
1. Vulnerability scans must be performed when new vulnerabilities, risks, or threats potentially affecting the system/applications are identified and reported.
2. Raw results from vulnerability scanning tools must be available in an unaltered format to the organization,
3. The organization must provide timely responses to informational requests for organizational monitoring status and security posture information.</td><td colspan="2"><b>RA-05: Vulnerability Monitoring and Scanning</b>
a. Monitor and scan for vulnerabilities in the system and hosted applications every thirty (30) calendar days and when new vulnerabilities potentially affecting the system are identified and reported;
b. Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
1. Enumerating platforms, software flaws, and improper configurations;
2. Formatting checklists and test procedures; and
3. Measuring vulnerability impact;
c. Analyze vulnerability scan reports and results from vulnerability monitoring;
d. Remediate legitimate vulnerabilities as follows: 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 one (1) year in accordance with the organization’s assessment of risk;
e. Share information obtained from the vulnerability monitoring process and control assessments with affected/related stakeholders to eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies); and
f. Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned.</td></tr>
</table>

EDE		ARC-AMPE	
4. Remediates all other findings (e.g., improper configurations, security controls not implemented, etc.) as follows; 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.			
Control	**Update Tool Capability**	**Control**	**N/A**
RA-5 (1): Update Tool Capability The organization employs vulnerability scanning tools that include the capability to readily update the information system vulnerabilities scanned.		**Withdrawn Control**: Incorporated into **RA-5**.	
Control	**Update by Frequency/Prior to New Scan/ When Identified**	**Control**	**Update Vulnerabilities to be Scanned**
RA-5 (2): Update by Frequency/Prior to New Scan/When Identified The organization updates the information system vulnerabilities scanned within every thirty (30) days, no less often than before each scan or when new vulnerabilities are identified and reported.		**RA-05(02): Update Vulnerabilities to be Scanned** Update the system vulnerabilities to be scanned prior to a new scan, and when new vulnerabilities are identified and reported.	
Control	**Privileged Access**	**Control**	**Privileged Access**
RA-5 (5): Privileged Access The information system implements privileged access authorization to operating system, telecommunications, and configuration components for selected vulnerability scanning activities to facilitate more thorough scanning. **Implementation Standards** 1. If Automated scanning tool functionality is used, it must be able to perform credentialed scans. 2. Credentialed scanning must be performed on all information systems and network devices (including appliances) 3. The organization must maintain and provide changes to the system accounts to support credentialed scanning no later than two (2) weeks prior to expiration or when other changes to the accounts are needed.		**RA-05(05): Privileged Access** Implement privileged access authorization to all components that support authentication for all scans.	
Control	**N/A**	**Control**	**Risk Response**
New NIST SP 800-53 Rev. 5 Control and applicable to ARC-AMPE		**RA-07: Risk Response** Respond to findings from security and privacy assessments, monitoring, and audits in accordance with organizational risk tolerance.	

EDE		ARC-AMPE	
Control	**N/A**	**Control**	**Privacy Impact Assessments**
New NIST SP 800-53 Rev. 5 Control and applicable to ARC-AMPE		**RA-08: Privacy Impact Assessments** Conduct privacy impact assessments for systems, programs, or other activities before: a. Developing or procuring information technology that processes Personally Identifiable Information (PII); and b. Initiating a new collection of PII that: 1. Will be processed using information technology; and 2. Includes PII permitting the physical or virtual (online) contact of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, ten (10) or more persons, other than agencies, instrumentalities, or employees of the federal government.	

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 (Risk Assessment (RA))_07142025