COALFIRE

WHITE PAPER

Migration from EDE to ARC-AMPE Planning (PL) controls

CMS requirements for Direct Enrollment Entities

IAN WALTERS, PRINCIPAL
JESSICA PAYNE, CONSULTANT

Table of contents

Purpose ..... Error! Bookmark not defined.
Background ..... Error! Bookmark not defined.
Affordable Care Act ..... **Error! Bookmark not defined.**
Enhanced Direct Enrollment ..... **Error! Bookmark not defined.**
CMS oversight ..... **Error! Bookmark not defined.**
ARC-AMPE ..... **Error! Bookmark not defined.**
Control mapping ..... Error! Bookmark not defined.
Planning (PL) 5
References **8**
Legal disclaimer **9**

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 Planning 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 (This Document)	**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.

Planning (PL)

The set of controls in this family focus on how the Exchange shall develop, document, periodically update, and implement security plans for Exchange IT systems that describe the security controls in place or planned for the IT systems and the rules of behavior for individuals accessing the IT systems.

<table>
<tr><th colspan="2">EDE</th><th colspan="2">ARC-AMPE</th></tr>
<tr><td><b>Control</b></td><td><b>Security Planning Policy and Procedures</b></td><td><b>Control</b></td><td><b>Policy and Procedures</b></td></tr>
<tr><td colspan="2"><b>PL-1: Security Planning Policy and Procedures</b>
The organization:
<b>a.</b> Develops, documents, and disseminates to applicable personnel:
<b>1.</b> A security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
<b>2.</b> Procedures to facilitate the implementation of the security planning policy and associated security planning controls.
<b>b.</b> Reviews and updates (as necessary) the current:
<b>1.</b> Security planning policy within every three (3) years; and
<b>2.</b> Security planning procedures within every three (3) years.
<b>Implementation Standards</b>
The organization retains the policies and procedures in written form (which may be electronic) for 6 years from the date of its creation or the date when it was last in effect, whichever is later. The organization makes the documentation available to those persons responsible for implementing the procedures to which the document pertains.</td><td colspan="2"><b>PL-01 Policy and Procedures</b>
<b>a.</b> Develop, document, and disseminate to organization-defined personnel or roles:
<b>1.</b> Organization-level planning policy that:
<b>(a)</b> Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
<b>(b)</b> Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines; and
<b>2.</b> Procedures to facilitate the implementation of the planning policy and the associated planning controls;
<b>b.</b> Designate an organization-defined official to manage the development, documentation, and dissemination of the planning policy and procedures; and
<b>c.</b> Review and update the current planning:
<b>1.</b> Policy at least every one (1) year and following organization-defined events; and
<b>2.</b> Procedures at least every one (1) year and following organization-defined events.</td></tr>
<tr><td><b>Control</b></td><td><b>System Security Plan</b></td><td><b>Control</b></td><td><b>System Security and Privacy Plan</b></td></tr>
<tr><td colspan="2"><b>PL-2: System Security Plan</b>
The organization:
<b>a.</b> Develops a security plan for the information system that:
<b>1.</b> Is consistent with CMS specified System Security and Privacy Plan (SSPP) Workbook;
<b>2.</b> Is consistent with the organization’s enterprise architecture;
<b>3.</b> Explicitly defines the authorization boundary for the system;
<b>4.</b> Describes the operational context of the information system in terms of missions and business processes;
<b>5.</b> Describes the operational environment for the information system and relationships with or connections to other information systems;
<b>6.</b> Provides an overview of the security requirements for the system;
<b>7.</b> Provides the security category
<b>8.</b> Personally Identifiable information (PII) confidentiality impact level of the system (as described in NIST SP 800-122),</td><td colspan="2"><b>PL-02 System Security and Privacy Plan</b>
<b>a.</b> Develop security and privacy plans for the system that:
<b>1.</b> Are consistent with the organization’s enterprise architecture;
<b>2.</b> Explicitly define the constituent system components;
<b>3.</b> Describe the operational context of the system in terms of mission and business processes;
<b>4.</b> Identify the individuals that fulfill system roles and responsibilities;
<b>5.</b> Identify the information types processed, stored, and transmitted by the system;
<b>6.</b> Provide the security categorization of the system, including supporting rationale;
<b>7.</b> Describe any specific threats to the system that are of concern to the organization;
<b>8.</b> Provide the results of a privacy risk assessment for systems processing Personally Identifiable Information (PII);</td></tr>
</table>

EDE		ARC-AMPE	
9. Describes relationships with, and data flows of, PII to other systems; and provide an overview of security and privacy requirements for the system **10.** Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions; and **11.** Is reviewed and approved by the authorizing official or designated representative prior to plan implementation; **b.** Distributes copies of the security plan and communicates subsequent changes to the plan to stakeholders; **c.** Reviews the security plan for the information system within every three hundred sixty-five (365) days; **d.** Updates the plan, at a minimum every three (3) years, to address current conditions or whenever: 1. There are significant changes to the information system/environment of operation that affect security; 2. Problems are identified during plan implementation or security control assessments; 3. When the data sensitivity level increases; 4. After a serious security violation due to changes in the threat environment; or 5. Before the previous security authorization expires; and **e.** Protects the security plan from unauthorized disclosure and modification. **Implementation Standard** The SSPP must define the boundary within the system where PII is stored, processed, and/or maintained. The person responsible for meeting information system privacy requirements must provide input to the SSPP.		**9.** Describe the operational environment for the system and any dependencies on or connections to other systems or system components; **10.** Provide an overview of the security and privacy requirements for the system; **11.** Identify any relevant control baselines or overlays, if applicable; **12.** Describe the controls in place or planned for meeting the security and privacy requirements, including a rationale for any tailoring decisions; **13.** Include risk determinations for security and privacy architecture and design decisions; **14.** Include security- and privacy-related activities affecting the system that require planning and coordination with organization-defined individuals or groups; and **15.** Are reviewed and approved by the Authorizing Official (AO) or designated representative prior to plan implementation. **b.** Distribute copies of the plans and communicate subsequent changes to the plans to organization-defined personnel, roles, or stakeholders; **c.** Review the plans at least every one (1) year or following significant changes; **d.** Update the plans to address changes to the system and environment of operation or problems identified during plan implementation or control assessments; and **e.** Protect the plans from unauthorized disclosure and modification.	
Control	**Plan/Coordinate with Other Organizational Entities**	**Control**	**N/A**
PL-2 (3): Plan/Coordinate with Other Organizational Entities The organization plans and coordinates security-related activities regarding the information system with affected stakeholders before conducting such activities to reduce the impact on other organizational entities.		Withdrawn. Incorporated into **PL-2**.	
Control	**Rules of Behavior**	**Control**	**Rules of Behavior**
PL-4: Rules of Behavior The organization: **a.** Establishes and makes readily available to individuals requiring access to the information system the rules that describe their responsibilities and expected behavior with regard to information and information system usage; **b.** Receives an acknowledgment (paper or electronic) from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior before authorizing access to information and the information system; **c.** Reviews the rules of behavior every three hundred sixty-five (365) days, updating if necessary; and		**PL-04 Rules of Behavior** **a.** Establish and provide to individuals requiring access to the system the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy; **b.** Receive a documented acknowledgment from such individuals, indicating that they have read, understood, and agree to abide by the rules of behavior, before authorizing access to information and the system; **c.** Review and update the rules of behavior at least every one (1) year; and **d.** Require individuals who have acknowledged a previous version of the rules of behavior to read and re-acknowledge when the rules are revised or updated.	

<table>
<tr><th colspan="2">EDE</th><th colspan="2">ARC-AMPE</th></tr>
<tr><td colspan="2"><b>d.</b> Requires individuals who have acknowledged a previous version of the rules of behavior to read and re-acknowledge when the rules of behavior are revised/updated.
<b>e.</b> Informs employees and contractors that the use of the organization’s information resources for anything other than authorized purposes set forth in the RoB is a violation of the policy, and is grounds for disciplinary action, monetary fines, and/or criminal charges that could result in imprisonment; and
<b>f.</b> Informs employees and contractors that the use of the organization’s information resources is subject to the organization’s monitoring of employee use of organizational information resources.</td><td colspan="2"></td></tr>
<tr><td><b>Control</b></td><td><b>Social Media and Networking Restrictions</b></td><td><b>Control</b></td><td><b>Social Media and External Site / Application Usage Restrictions</b></td></tr>
<tr><td colspan="2"><b>PL-4 (1): Social Media and Networking Restrictions</b>
The organization includes in the rules of behavior explicit restrictions on the use of social media/networking sites and posting organizational information on public websites.</td><td colspan="2"><b>PL-04(01) Social Media and External Site / Application Usage Restrictions</b>
Include in the rules of behavior restrictions on:
<b>a.</b> Use of social media, social networking sites, and external sites/applications;
<b>b.</b> Posting organizational information on public websites; and
<b>c.</b> Use of organization-provided identifiers (e.g., email addresses) and authentication secrets (e.g., passwords) for creating accounts on external sites/applications.</td></tr>
<tr><td><b>Control</b></td><td><b>Information Security Architecture</b></td><td><b>Control</b></td><td><b>Security and Privacy Architectures</b></td></tr>
<tr><td colspan="2"><b>PL-8: Information Security Architecture</b>
The organization:
<b>a.</b> Develops an information security architecture for the ACA system that:
<b>1.</b> Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information;
<b>2.</b> Describes how the information security architecture is integrated into and supports the enterprise architecture;
<b>3.</b> Describes any information security assumptions about, and dependencies on, external services;
<b>b.</b> Reviews and updates (as necessary) the information security architecture whenever changes are made to the enterprise architecture; and
<b>c.</b> Ensures that planned information security architecture changes are reflected in the security plan and organizational procurements/acquisitions.</td><td colspan="2"><b>PL-08 Security and Privacy Architectures</b>
<b>d.</b> Develop security and privacy architectures for the system that:
<b>4.</b> Describe the requirements and approach to be taken for protecting the confidentiality, integrity, and availability of organizational information;
<b>5.</b> Describe the requirements and approach to be taken for processing Personally Identifiable Information (PII) to minimize privacy risk to individuals;
<b>6.</b> Describe how the architectures are integrated into and support the enterprise architecture; and
<b>7.</b> Describe any assumptions about, and dependencies on, external systems and services;
<b>e.</b> Review and update the architectures at least every one (1) year or following a significant change to reflect changes in the enterprise architecture; and
<b>f.</b> Reflect planned architecture changes in security and privacy plans, Concept of Operations (CONOPS), criticality analysis, organizational procedures, and procurements and acquisitions.</td></tr>
<tr><td><b>Control</b></td><td><b>N/A</b></td><td><b>Control</b></td><td><b>Baseline Tailoring</b></td></tr>
<tr><td colspan="2">New NIST SP 800-53 Rev. 5 Control and applicable to ARC-AMPE</td><td colspan="2"><b>PL-11: Baseline Tailoring</b>
Tailor the selected control baseline by applying specified tailoring actions.</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

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.

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.

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 (Planning (PL))_07142025