COALFIRE

WHITE PAPER

Migration from EDE to ARC-AMPE Physical and Environmental Protection (PE) 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 Physical and Environment 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	8
Physical and Environmental Protection (This Document)	**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.

Physical and Environmental Protection (PE)

The set of controls in this family focus on how the exchange shall: (1) limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (2) protect the physical plant and support infrastructure for information systems; (3) provide supporting utilities for information systems; (4) protect information systems against environmental hazards; and (5) provide appropriate environmental controls in facilities containing information systems.

EDE		ARC-AMPE	
Control	**Physical and Environmental Protection Policy and Procedures**	**Control**	**Policy and Procedures**
PE-1: Physical and Environmental Protection Policy and Procedures The organization: **a.** Develops, documents, and disseminates to applicable personnel: **1.** A physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and **2.** Procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls. **b.** Reviews and updates (as necessary) the current: **1.** Physical and environmental protection policy within every three (3) years; and **2.** Physical and environmental protection procedures within every three (3) years.		**PE-01: Policy and Procedures** **a.** Develop, document, and disseminate to applicable personnel or roles: **1.** Organization-level physical and environmental protection 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 physical and environmental protection policy and the associated physical and environmental protection controls; **b.** Designate an organization-defined official to manage the development, documentation, and dissemination of the physical and environmental protection policy and procedures; and **c.** Review and update the current physical and environmental protection: **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.	

EDE		ARC-AMPE	
Control	**Physical Access Authorizations**	**Control**	**Physical Access Authorizations**
PE-2: Physical Access Authorizations The organization: **a.** Develops and maintains a current list of individuals with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible); **b.** Issues authorization credentials; and **c.** Reviews and approves the access list detailing authorization credentials every one hundred eighty (180) days, removing from the access list those personnel no longer requiring access. **Implementation Standards** **1.** Review and approve lists of personnel with authorized access to facilities containing information systems at least once every one hundred eighty (180) days. **2.** Create a restricted area, security room, or locked room to control access to areas containing Personally Identifiable Information (PII). These areas will be controlled accordingly.		**PE-02: Physical Access Authorizations** **a.** Develop, approve, and maintain a list of individuals with authorized access to the facility where the system resides; **b.** Issue authorization credentials for facility access; **c.** Review the access list detailing authorized facility access by individuals at least every six (6) months; and **d.** Remove individuals from the facility access list when access is no longer required.	
Control	**Access by Position / Role**	**Control**	**N/A**
PE-2(1): Access by Position / Role The organization authorizes physical access to the facility where the information system resides based on position or role.		**Withdrawn Control**: No longer required for the minimum baseline but should still be considered a best practice.	
Control	**Physical Access Control**	**Control**	**Physical Access Control**
PE-3: Physical Access Control The organization: **a.** Enforces physical access authorizations at defined entry/exit points to the facility (defined in the applicable security plan) where the information system resides by: **1.** Verifying individual access authorizations before granting access to the facility; and **2.** Controlling ingress/egress to the facility using guards and/or defined physical access control systems/devices (defined in the applicable security plan). **b.** Maintains physical access audit logs for defined entry/exit points; **c.** Escorts visitors and monitors visitor activity in defined circumstances requiring visitor escorts and monitoring (defined in the applicable security plan); **d.** Secures keys, combinations, and other physical access devices; **e.** e. Inventories physical access devices within every 90 days: and **f.** Changes combinations and keys for defined high-risk entry/exit points (defined in the applicable security plan) within every three hundred sixty-five (365) days, and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.		**PE-03: Physical Access Control** **a.** Enforce physical access authorizations at entry and exit points to the facility where the system resides by: **1.** Verifying individual access authorizations before granting access to the facility; and **2.** Controlling ingress and egress to the facility using organization-defined physical access control systems or devices and/or guards; **b.** Maintain physical access audit logs for entry or exit points; **c.** Control access to areas within the facility designated as publicly accessible by implementing the following controls: organization-defined security safeguards or physical access controls; **d.** Escort visitors and control visitor activity in organization-defined circumstances requiring visitor escorts and controlling of visitor activity; **e.** Secure keys, combinations, and other physical access devices; **f.** Inventory organization-defined physical access devices every ninety (90) days; and **g.** Change combinations and keys at least every one (1) year or earlier as required by a security-relevant event and/or when keys are lost, combinations are compromised, or when individuals possessing the keys or combinations are transferred or terminated.	

<table>
<tr><th colspan="2">EDE</th><th colspan="2">ARC-AMPE</th></tr>
<tr><td colspan="2">Implementation Standards
1. Control data center/facility access by use of door and window locks and security personnel or physical authentication devices, such as biometrics and/or smart card/PIN combination.
2. Store and operate servers in physically secure environments and grant access to explicitly authorized personnel only. Access is monitored and recorded.
3. Restrict access to grounds/facilities to authorized persons only.
4. Require two barriers to access PII under normal security: secured perimeter/locked container, locked perimeter/secured interior, or locked perimeter/security container. Protected information must be containerized in areas where other than authorized employees may have access afterhours.</td><td colspan="2"></td></tr>
<tr><td>Control</td><td>Access Control for Transmission</td><td>Control</td><td>Access Control for Transmission</td></tr>
<tr><td colspan="2">PE-4: Access Control for Transmission Medium
The organization controls physical access to information system distribution and transmission lines within organizational facilities.
Implementation Standards
Disable any physical ports (e.g., wiring closets and patch panels) not in use.</td><td colspan="2">PE-04: Access Control for Transmission
Control physical access to organization-defined system distribution and transmission lines within organizational facilities using organization-defined security controls or safeguards.</td></tr>
<tr><td>Control</td><td>Access Control for Output Devices</td><td>Control</td><td>Access Control for Output Devices</td></tr>
<tr><td colspan="2">PE-5: Access Control for Output Devices
The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.</td><td colspan="2">PE-05: Access Control for Output Devices
Control physical access to output from organization-defined output devices to prevent unauthorized individuals from obtaining the output.</td></tr>
<tr><td>Control</td><td>Monitoring Physical Access</td><td>Control</td><td>Monitoring Physical Access</td></tr>
<tr><td colspan="2">PE-6: Monitoring Physical Access
The organization:
a. Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents;
b. Reviews physical access logs at least semi-annually and upon occurrence of security incidents involving physical security; and
c. Coordinates results of reviews and investigations with the organization's incident response capability
Implementation Standard
The organization reviews physical access logs at least semi-annually.</td><td colspan="2">PE-06: Monitoring Physical Access
a. Monitor physical access to the facility where the system resides to detect and respond to physical security incidents;
b. Review physical access logs at least monthly (every thirty [30] days) and upon occurrence of organization-defined events or potential indications of events; and
c. Coordinate results of reviews and investigations with the organizational incident response capability.</td></tr>
<tr><td>Control</td><td>Intrusion Alarms/Surveillance Equipment</td><td>Control</td><td>Intrusion Alarms and Surveillance Equipment</td></tr>
<tr><td colspan="2">PE-6 (1): Intrusion Alarms/Surveillance Equipment
The organization monitors physical intrusion alarms and surveillance equipment.</td><td colspan="2">PE-06(01): Intrusion Alarms and Surveillance Equipment
Monitor physical access to the facility where the system resides using physical intrusion alarms and surveillance equipment.</td></tr>
</table>

EDE		ARC-AMPE	
Control	**Visitor Access Records**	**Control**	**Visitor Access Records**
PE-8: Visitor Access Records The organization: **a.** Maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) for two (2) years; and **b.** Reviews visitor access records at least monthly. **Implementation Standards** At a minimum, visitor access records must include the following information: **1.** Name and organization of the person visiting; **2.** Visitor's signature; **3.** Form of identification; **4.** Date of access; **5.** Time of entry and departure; **6.** Purpose of visit; and **7.** Name and organization of person visited.		**PE-08: Visitor Access Records** **a.** Maintain visitor access records to the facility where the system resides for at least one (1) year; **b.** Review visitor access records at least monthly (every thirty [30] days); and **c.** Report anomalies in visitor access records to organization-defined personnel or roles.	
Control	**N/A**	**Control**	**Delivery and Removal**
Existing NIST SP 800-53 Rev.4 control and new to ARC-AMPE.		**PE-08: Delivery and Removal** **d.** Authorize and control all system components entering and exiting the facility; and **e.** Maintain records of the system components.	

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 (Physical and Environmental Protection (PE))_07142025