COALFIRE

WHITE PAPER

Migration from EDE to ARC-AMPE Personnel Security (PS) 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 ..... 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.
Personnel Security (PS) 5
References **9**
Legal disclaimer **10**

Purpose

This white paper provides a guide for Direct Enrollment Entities (DEEs) to upgrade their Enhanced Direct Enrollment (EDE) System Security and Privacy Plans (SSPPs) to the Acceptable Risk Controls for ACA, Medicaid, and Provider Entities (ARC-AMPE).

Due to the substantial number of controls, and to facilitate ease of use, this white paper is one of a series of 20 which divides the ARC-AMPE by control family. This white paper addresses the Personnel Security 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 (This Document)	**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.

Personnel Security (PS)

The set of controls in this family focus on how the Exchange shall: (1) ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions; (2) ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers; and (3) employ formal sanctions for personnel failing to comply with organizational security policies and procedures.

EDE		ARC-AMPE	
Control	**Personnel Security Policy and Procedures**	**Control**	**Policy and Procedures**
PS-1: Personnel Security Policy and Procedures The organization: **a.** Develops, documents, and disseminates to applicable personnel: **1.** A personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and **2.** Procedures to facilitate the implementation of the personnel security policy and associated personnel security controls. **b.** Reviews and updates (as necessary) the current: **1.** Personnel security policy within every three (3) years; and **2.** Personnel security procedures within every three (3) years.		**PS-01: Policy and Procedures** **a.** Develop, document, and disseminate to applicable personnel and roles: **1.** Organization-level personnel security 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 personnel security policy and the associated personnel security 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 personnel security: **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	**Position Risk Designation**	**Control**	**Position Risk Designation**
PS-2: Position Risk Designation The organization: a. Assigns a criticality/sensitivity risk designation to all organizational positions; b. Establishes screening criteria for individuals filling those positions; and c. Reviews and revises position criticality/sensitivity risk designations within every three years.		**PS-02: Position Risk Designation** **a.** Assign a risk designation to all organizational positions; **b.** Establish screening criteria for individuals filling those positions; and **c.** Review and update position risk designations at least every one (1) year or whenever a position's duties are changed, revised, or realigned.	
Control	**Personnel Screening**	**Control**	**Personnel Screening**
PS-3: Personnel Screening The organization: a. Screens individuals prior to authorizing access to the information system; b. Rescreens individuals periodically, consistent with the criticality/sensitivity risk designation of the position; and		**PS-03: Personnel Screening** **a.** Screen individuals prior to authorizing access to the system; and **b.** Rescreen individuals in accordance with organizational Personnel Security Policy and anytime they change a position.	

EDE	ARC-AMPE
c. When an employee moves from one position to another, the higher level of clearance should be adjudicated. **Implementation Standards** 1. Perform criminal history check for all persons prior to employment. 2. All employees and contractors requiring access to ACA-sensitive information must meet personnel suitability standards. These suitability standards are based on a valid need-to-know, which cannot be assumed from position or title, and favorable results from a background check. The background check for prospective and existing employees (if not previously completed) should include, at a minimum, contacting references provided by the employee as well as the local law enforcement agency or agencies.	
Control **Personnel Termination**	**Control** **Personnel Termination**
PS-4: Personnel Termination The organization, upon termination of individual employment: **a.** Disables information system access in accordance with Implementation Standard 1; **b.** Terminates/revokes any authenticators/credentials associated with the individual; **c.** Conducts exit interviews that include a discussion of non-disclosure of information security and privacy information; **d.** Retrieves all security-related organizational information system-related property; **e.** Retains access to organizational information and information systems formerly controlled by a terminated individual; **f.** Notifies defined personnel or roles (defined in the applicable security plan) within one (1) business day; and **g.** Immediately escorts employees terminated for cause out of the organization. **Implementation Standards** **1.** System and physical access must be revoked prior to or during the employee termination process. **2.** All access and privileges to systems, networks, and facilities are suspended when employees or contractors temporarily separate from the organization (e.g., leave of absence).	**PS-04: Personnel Termination** Upon termination of individual employment: **a.** Disable system access within the same day as termination; **b.** Terminate or revoke any authenticators and credentials associated with the individual; **c.** Conduct exit interviews that include a discussion of non-disclosure of information security and privacy information; **d.** Retrieve all security-related organizational system-related property; and **e.** Retain access to organizational information and systems formerly controlled by the terminated individual.
Control **Personnel Transfer**	**Control** **Personnel Transfer**
PS-5: Personnel Transfer The organization: **a.** Reviews and confirms ongoing operational need for current logical and physical access authorizations to information systems/facilities when personnel are reassigned or transferred to other positions within the organization;	**PS-05: Personnel Transfer** **a.** Review and confirm ongoing operational need for current logical and physical access authorizations to systems and facilities when individuals are reassigned or transferred to other positions within the organization; **b.** Initiate reassignment actions to ensure all system accesses no longer required (e.g., need to know) are removed or disabled within twenty-four (24) hours:

EDE	ARC-AMPE
b. Initiates the following transfer or reassignment actions during the formal transfer process: **1.** Re-issuing appropriate information system-related property (e.g., keys, identification cards, and building passes); **2.** Notifying security management; **3.** Closing obsolete accounts and establishing new accounts; **4.** When an employee moves to a new position of trust, logical and physical access controls must be re-evaluated within five (5) days following the formal transfer action; **c.** Modifying access authorization as necessary to correspond with any changes in operational need due to reassignment or transfer; and **d.** Notifying defined personnel or roles (defined in the applicable security plan) within one (1) business day.	**c.** Modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and **d.** Notify organization-defined personnel or roles within twenty-four (24) hours.
Control **Access Agreements**	**Control** **Access Agreements**
PS-6: Access Agreements The organization: **a.** Develops and documents access agreements for organizational information systems, consistent with the provisions of the ACA and the requirements of 45 CFR §155.260 – Privacy and security of personally identifiable information, paragraphs (b)(2) and (c). **b.** Reviews and updates the access agreements as part of the system security authorization or when a contract is renewed or extended, but minimally within every three hundred sixty-five (365) days, whichever occurs first; and **c.** Ensures that individuals requiring access to organizational information and information systems: **1.** Acknowledge (paper or electronic) appropriate access agreements prior to being granted access; and **2.** Re-acknowledge access agreements to maintain access to organizational information systems when access agreements have been updated or within every 365 days.	**PS-06: Access Agreements** **a.** Develop and document access agreements for organizational systems; **b.** Review and update the access agreements as part of the system security authorization or when a contract is renewed or extended, but at a minimum at least every one (1) year; and **c.** Verify that individuals requiring access to organizational information and systems: **1.** Sign appropriate access agreements (paper or electronic) prior to being granted access; and **2.** Re-sign access agreements to maintain access to organizational systems when access agreements have been updated or at least every one (1) year.
Control **Third-Party Personnel Security**	**Control** **External Personnel Security**
PS-7: Third-Party Personnel Security The organization: **a.** Establishes personnel security requirements including security roles and responsibilities for third-party providers; **b.** Requires third-party providers to comply with personnel security policies and procedures established by the organization; **c.** Documents personnel security requirements; **d.** Requires third-party providers to notify Contracting Officers or Contracting Officer's Representatives (via the roster of contractor personnel) of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within seven (7) calendar days; and	**PS-07: External Personnel Security** **a.** Establish personnel security requirements, including security roles and responsibilities for external providers; **b.** Require external providers to comply with personnel security policies and procedures established by the organization; **c.** Document personnel security requirements; **d.** Require external providers to notify organization-defined personnel or roles of any personnel transfers or terminations of external personnel who possess organizational credentials and/or badges, or who have system privileges within twenty-four (24) hours; and **e.** Monitor provider compliance with personnel security requirements.

<table>
<tr><th colspan="2">EDE</th><th colspan="2">ARC-AMPE</th></tr>
<tr><td colspan="2">e. Monitors provider compliance.

Implementation Standards
Regulate the access provided to contractors and define security requirements for contractors. Contractors must be provided with minimal system and physical access and must agree to and support the information security requirements. The contractor selection process must assess the contractor’s ability to adhere to and support information security policies and standards.</td><td colspan="2"></td></tr>
<tr><td>Control</td><td>Personnel Sanctions</td><td>Control</td><td>Personnel Sanctions</td></tr>
<tr><td colspan="2">PS-8: Personnel Sanctions
The organization:
a. Employs a formal sanctions process for individuals failing to comply with established information security policies and procedures; and
b. Notifies defined personnel or roles (defined in the applicable security plan) within defined time period (defined in the applicable security plan) not to exceed seven (7) calendar days when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction..</td><td colspan="2">PS-08: Personnel Sanctions
a. Employ a formal sanctions process for individuals failing to comply with established information security and privacy policies and procedures; and
b. Notify organization-defined personnel or roles within twenty-four (24) hours when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.</td></tr>
</table>

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 (Personnel Security (PS))_07142025