COALFIRE

WHITE PAPER

Migration from EDE to ARC-AMPE Awareness and Training (AT) 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 Awareness and Training controls.

ARC-AMPE Control Families	
Control Family	**Number of Controls**
Access Control	46
Awareness and Training (This Document)	**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	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.

Awareness and Training (AT)

The set of controls in this family focus on how the Exchange shall: (1) ensure that managers and users of Exchange IT systems are made aware of the security risks associated with their activities and of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures related to the security of IT systems; and (2) ensure that Exchange personnel are adequately trained to carry out their assigned Information Security related duties and responsibilities.

EDE		ARC-AMPE	
Control	**Security Awareness and Training Policy and Procedures**	**Control**	**Policy and Procedures**
AT-1: Security Awareness and Training Policy and Procedures The organization: a. Develops, documents, and disseminates to personnel/roles as designated by the organization: 1. A security awareness and training 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 awareness and training policy and associated security awareness and training controls; and b. Reviews and, if necessary, updates the current: 1. Security awareness and training policy at least once every three (3) years; and 2. Security awareness and training procedures at least once every three (3) years.		**AT-01 Policy and Procedures** **a.** Develop, document, and disseminate to applicable personnel or roles: **1.** Organization-level awareness and training 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 awareness and training policy and the associated awareness and training controls; **b.** Designate an organization-defined official to manage the development, documentation, and dissemination of the awareness and training policy and procedures; and **c.** Review and update the current awareness and training: **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 Awareness Training**	**Control**	**Literacy Training and Awareness**
AT-2: Security Awareness Training The organization provides basic security and privacy awareness training to information system users (including managers, senior executives, and contractors): a. As part of initial training for new users prior to accessing any system's information; b. When required by system changes, and c. within every three hundred sixty-five (365) days thereafter. **Implementation Standards** 1. An information security and privacy education and awareness training program is developed and implemented for all employees and contractors working on behalf of the organization and involved in accessing, using, managing or developing information systems. 2. Information security and privacy education awareness training must address individuals’		**AT-02: Literacy Training and Awareness** **a.** Provide security and privacy literacy training to system users (including managers, senior executives, and contractors): **1.** As part of initial training for new users and within at least every one (1) year thereafter; and **2.** When required by system changes or following organization-defined events; **b.** Employ the following techniques to increase the security and privacy awareness of system users: phishing email tests and other organization-defined techniques. **c.** Update literacy training and awareness content at least once every one (1) year and following organization-defined events; and **d.** Incorporate lessons learned from internal or external security incidents or breaches into literacy training and awareness techniques.	

EDE		ARC-AMPE	
responsibilities associated with sending sensitive information in email. **3.** Security and privacy awareness training is provided before granting access to systems and networks, and within every three hundred sixty-five (365) days thereafter, to all employees and contractors to explain the importance and responsibility in safeguarding Personally Identifiable Information (PII) and ensuring privacy as established in federal legislation and OMB guidance.			
Control	**Insider Threat**	**Control**	**Insider Threat**
AT-2 (2): Insider Threat The organization includes security and privacy awareness training on recognizing and reporting potential indicators of insider threats, such as: **a.** Inordinate, long-term job dissatisfaction; **b.** Attempts to gain access to information not required for job performance; **c.** Unexplained access to financial resources; **d.** Bullying or sexual harassment of fellow employees; **e.** Workplace violence; and **f.** Other serious violations of organizational policies, procedures, directives, rules, or practices. **Implementation Standards** Security awareness training includes how to communicate employee and management concerns regarding potential indicators of insider threat through appropriate organizational channels in accordance with established organizational policies and procedures.		**AT-02(02): Insider Threat** Provide literacy training on recognizing and reporting potential indicators of insider threat.	
Control	**N/A**	**Control**	**Social Engineering and Mining**
New NIST SP 800-53 Rev.5 control and applicable to ARC-AMPE.		**AT-02(03): Social Engineering and Mining** Provide literacy training on recognizing and reporting potential and actual instances of social engineering and social mining.	
Control	**N/A**	**Control**	**Suspicious Communications and Anomalous System Behavior**
• New NIST SP 800-53 Rev.5 control and applicable to ARC-AMPE • Withdrawn control **AT-3(4)**.		**AT-02(04): Suspicious Communications and Anomalous System Behavior** Provide literacy training on recognizing suspicious communications and anomalous behavior in organizational systems using organization-defined indicators of malicious code.	
Control	**N/A**	**Control**	**Advanced Persistent Threat**
New NIST SP 800-53 Rev.5 control and applicable to ARC-AMPE.		**AT-02(05): Advanced Persistent Threat** Provide literacy training on the advanced persistent threat (APT).	

EDE		ARC-AMPE	
Control	**Role-Based Security Training**	**Control**	**Role-Based Training**
AT-3: Role-Based Security Training The organization provides role-based security and privacy training to personnel (both contractor and employee) with assigned security and privacy roles and responsibilities: a. Before authorizing access to the information system or performing assigned duties; and b. When required by information system changes; and c. Within sixty (60) days of entering a position that requires role-specific training, within every three hundred sixty-five (365) days thereafter. **Implementation Standards** 1. Require personnel with significant information security and privacy roles and responsibilities to undergo appropriate information system security and privacy training prior to authorizing access to networks, systems, and/or applications; when required by significant information system or system environment changes; when an employee enters a new position that requires additional role-specific training; and for refresher training within every three hundred sixty-five (365) days thereafter. **2.** All personnel with significant information security roles and responsibilities that have not completed the required training within the mandated timeframes shall have their user accounts disabled until they have met their role-based training requirement		**AT-03: Role-Based Training** **a.** Provide role-based security and privacy training to personnel with the following significant information security and privacy roles and responsibilities: **1.** Before authorizing access to the system, information, or performing assigned duties, and at least every one (1) year thereafter; and **2.** When required by system changes; **b.** Update role-based training (RBT) content at least every one (1) year and following significant changes to the system or the system environment changes; and **c.** Incorporate lessons learned from internal or external security incidents or breaches into role-based training.	
Control	**N/A**	**Control**	**Processing Personally Identifiable Information**
• New NIST SP 800-53 Rev.5 control and applicable to ARC-AMPE • Training elements of withdrawn control **UL-2**.		**AT-03(05): Processing Personally Identifiable Information** Provide organizational-personnel (to include vendors, contractors, and employees) with initial, and at least every one (1) year thereafter, training in the employment and operation of Personally Identifiable Information (PII) processing and transparency controls.	
Control	**Security Training Records**	**Control**	**Training Records**
AT-4: Security Training Records The organization: **a.** Identifies employees and contractors who hold roles with significant information security and privacy responsibilities; **b.** Documents and monitors individual information system security and privacy training activities including basic security and privacy awareness training and specific information system security and privacy training; and **c.** Retains individual training records for a minimum of five (5) years after the individual completes each training.		**AT-04: Training Records** **a.** Document and monitor information security and privacy training activities, including security and privacy awareness training and specific role-based security and privacy training; and **b.** Retain individual training records for a minimum of five (5) years after completing a specific training course.	

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 (Awareness and Training)_07142025