COALFIRE

WHITE PAPER

Migration from EDE to ARC-AMPE Identification and Authentication (IA) 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 Identification and Authentication 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 (This Document)	**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.

Identification and Authentication (IA)

The set of controls in this family focus on how the Exchange shall identify IT system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to Exchange IT systems.

EDE		ARC-AMPE	
Control	**Identification and Authentication Policy and Procedures**	**Control**	**Policy and Procedures**
IA-1: Identification and Authentication Policy and Procedures The organization: **a.** Develops, documents, and disseminates to applicable personnel: **1.** An identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and **2.** Procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls. **b.** Reviews and updates (as necessary) the current: **1.** Identification and authentication policy at least every three (3) years; and **2.** Identification and authentication procedures at least every three (3) years.		**IA-01: Policy and Procedures** **a.** Develop, document, and disseminate to applicable personnel or roles: **1.** Organization-level identification and authentication 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 identification and authentication policy and the associated identification and authentication controls; **b.** Designate an organization-defined official to manage the development, documentation, and dissemination of the identification and authentication policy and procedures; and **c.** Review and update the current identification and authentication: **1.** Policy at least one (1) year and following organization-defined events; and **2.** Procedures at least every one (1) year and following organization-defined events.	
Control	**Identification and Authentication (Organizational Users)**	**Control**	**Identification and Authentication (Organizational Users)**
IA-2: Identification and Authentication (Organizational Users) The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users). **Implementation Standards** **1.** Require the use of system and/or network authenticators and unique user identifiers. **2.** Help desk support requires user identification for any transaction that has information security implications.		**IA-02: Identification and Authentication (Organizational Users)** Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.	
Control	**Network Access to Privileged Accounts**	**Control**	**Multifactor Access to Privileged Accounts**
IA-2 (1): Network Access to Privileged Accounts The information system implements multifactor authentication for network access to privileged accounts.		**IA-02(01): Multifactor Access to Privileged Accounts** Implement multi-factor authentication for access to privileged accounts.	

EDE		ARC-AMPE	
Control	**Network Access to Non-Privileged Accounts**	**Control**	**Multifactor Access to Non-Privileged Accounts**
IA-2 (2): Network Access to Non-Privileged Accounts The information system implements multifactor authentication for network access to non-privileged accounts.		**IA-02(02): Multifactor Access to Non-Privileged Accounts** Implement multi-factor authentication for access to non-privileged accounts.	
Control	**Local Access to Privileged Accounts**	**Control**	**N/A**
IA-2 (3): Local Access to Privileged Accounts The information system implements multifactor authentication for local access to privileged accounts.		**Withdrawn control**: Incorporated into **IA-02(01)**.	
Control	**N/A**	**Control**	**Access to Accounts - Separate Device**
Existing NIST SP 800-53 Rev.4 control and new to ARC-AMPE.		**IA-02(06): Access to Accounts - Separate Device** Implement multi-factor authentication for local, network, and remote access to privileged (IA-2(01)) and non-privileged accounts (IA-2(02)) such that: (a) One of the factors is provided by a device separate from the system gaining access; and (b) The device meets the most current FIPS 140-compliant cryptography.	
Control	**Network Access to Privileged Accounts – Replay Resistant**	**Control**	**Access to Accounts – Replay Resistant**
IA-2 (8): Network Access to Privileged Accounts – Replay Resistant The information system implements replay-resistant authentication mechanisms for network access to privileged accounts.		**IA-02(08): Access to Accounts – Replay Resistant** Implement replay-resistant authentication mechanisms for access to privileged and non-privileged accounts.	
Control	**Remote Access – Separate Device**	**Control**	**N/A**
IA-2 (11): Remote Access – Separate Device The information system implements multifactor authentication for remote access to privileged and non-privileged accounts, assuring that one of the factors is provided by a device separate from the system gaining access.		**Withdrawn control**: Incorporated into **IA-02(06)**.	
Control	**Device Identification and Authentication**	**Control**	**Device Identification and Authentication**
IA-3: Device Identification and Authentication The information system uniquely identifies and authenticates defined types of devices (defined in the applicable security plan) that require authentication mechanisms which, at a minimum, use shared information [Media Access Control (MAC) or Internet Protocol (IP) address] and access control lists to control remote network access prior to establishing the connection. If remote authentication is provided by the system itself, the system must follow most recent NIST SP 800-63 Digital Identify Guidelines. **Implementation Standards**		**IA-03: Device Identification and Authentication** Uniquely identify and authenticate devices that require authentication mechanisms, which, at a minimum, use shared information (Media Access Control [MAC] or Internet Protocol [IP] address) and access control lists to control remote network access before establishing a local, remote, or network connection.	

EDE	ARC-AMPE
The organization defines a list of specific devices and/or types of devices approved and accepted for identification and authentication management.	
Control **Identifier Management**	**Control** **Identifier Management**
IA-4: Identifier Management The organization manages information system identifiers by: **a.** Receiving authorization from organization-defined personnel or roles (defined in the applicable security plan) to assign an individual, group, role, or device identifier; **b.** Selecting an identifier that identifies an individual, group, role, or device; **c.** Assigning the identifier to the intended individual, group, role, or device; **d.** Preventing reuse of identifiers until all previous access authorizations are removed from the system, including all file accesses for that identifier but not before a period of three (3) years or more has passed; and **e.** Disabling the identifier after sixty (60) days or less of inactivity and deleting disabled accounts during the annual re-certification process. **Implementation Standards** **1.** The organization defines time period of inactivity for device identifiers. **2.** Social security numbers (SSNs), and parts of SSNs, must not be used as system identifiers. Identifier management must ensure that any access to, or action involving, personally identifiable information (PII) is attributable to a unique individual.	**IA-04: Identifier Management** Manage system identifiers by: **a.** Receiving authorization from organization-defined personnel or roles to assign an individual, group, role, service, or device identifier; **b.** Selecting an identifier that identifies an individual, group, role, service, or device; **c.** Assigning the identifier to the intended individual, group, role, service, or device; and **d.** Preventing reuse of identifiers for two (2) years.
Control **N/A**	**Control** **Identify User Status**
Existing NIST SP 800-53 Rev.4 control and new to ARC-AMPE.	**IA-04(04): Identify User Status** Manage individual identifiers by uniquely identifying each individual using one or more organization-defined characteristics identifying individual status.
Control **Authenticator Management**	**Control** **Authenticator Management**
IA-5: Authenticator Management The organization manages information system authenticators by: **a.** Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator. **b.** Establishing initial authenticator content for authenticators defined by the organization; **c.** Ensuring that authenticators have sufficient strength of mechanism for their intended use; **d.** Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;	**IA-05: Authenticator Management** Manage system authenticators by: **a.** Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator; **b.** Establishing initial authenticator content for any authenticators issued by the organization; **c.** Ensuring that authenticators have sufficient strength of mechanism for their intended use; **d.** Establishing and implementing administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators; **e.** Changing default authenticators prior to first use; **f.** Changing or refreshing authenticators:

EDE	ARC-AMPE
e. Changing default content of authenticators prior to information system installation; **f.** Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators; **g.** Changing/refreshing authenticators as follows: **1.** Passwords are valid for no longer than the period directed in IA-5 (1); immediately in the event of known or suspected compromise; and immediately upon system installation (e.g., default or vendor-supplied passwords); **2.** Public Key Infrastructure (PKI) certificates issued in accordance with the Federal PKI Common Policy are valid for no longer than three (3) years; **3.** Any PKI authentication request must be validated by Online Certificate Status Protocol (OCSP) or Certificate Revocation List (CRL) to ensure that the certificate being used for authentication has not been revoked. **4.** All other authenticator types every sixty (60) days; **h.** Protecting authenticator content from unauthorized disclosure and modification; **i.** Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and **j.** Changing authenticators for group/role accounts when membership to those accounts change.	– At least every one (1) year for User Account password; – At least every one (1) year and three (3) months for ACA Consumer Account password; or when authenticators: – Are no longer valid in the event of known or suspected compromise, and requiring immediate change; or – Must be changed immediately upon system installation (e.g., default or vendor-supplied passwords); **g.** Protecting authenticator content from unauthorized disclosure and modification; **h.** Requiring individuals to take, and having devices implement, specific controls to protect authenticators; and **i.** Changing authenticators for group or role accounts when membership to those accounts changes.
Control **Password-Based Authentication**	**Control** **Password-Based Authentication**
IA-5 (1): Password-Based Authentication For password-based authentication, the information systems follow the direction in the applicable configuration baselines per CM-6, or as follows, whichever is more stringent: **a.** Allows the use of a temporary password for system logons with an immediate change to a permanent password. **b.** Password Complexity: User Accounts: Enforces minimum password complexity of case sensitive, minimum of eight (8) characters, and at least one (1) each of upper-case letters, lower-case letters, numbers, and special characters; **c.** Prohibits the use of dictionary names or words; **d.** Enforces at least the following minimum password requirements for Users / Privileged Users / Processes [acting on behalf of a User] **1.** MinimumPasswordAge = 1/1/1/1; **2.** MaximumPasswordAge = 60/60/60 **3.** MinimumPasswordLength = 8/15/15 **e.** Enforces at least six (6) changed characters or as determined by the information system (where possible) when new passwords are created; **f.** Encrypts passwords in storage and in transmission; **g.** Prohibit password reuse for 24 generations; and **h.** Password-protect system initialization (boot) settings. **Implementation Standard**	**IA-05(01): Password-Based Authentication** For password-based authentication: **a.** Maintain a list of commonly used, expected, or compromised passwords and update the list using a frequency defined in applicable security/privacy plans, but not to exceed one (1) year, and when organizational passwords are suspected to have been compromised directly or indirectly; **b.** Verify, when users create or update passwords, that the passwords are not found on the organization and Mission/Business/System-defined lists of commonly used, expected, compromised passwords in IA-5(1)(a); **c.** Transmit only cryptographically protected channels; **d.** Store passwords using an approved salted key derivation function, preferably using a keyed hash; **e.** Require immediate selection of a new password upon account recovery; **f.** Allow user selection of long passwords and passphrases, including spaces and all printable characters; **g.** Employ automated tools to assist the user in selecting strong password authenticators; and **h.** Enforce the following composition and complexity rules: – At least 75 percent of the password changed when new passwords are created; – Prohibit password reuse for twenty-four (24) generations; and – Administrator/Privileged Accounts: Minimum password complexity of case sensitive, minimum of fifteen (15)

EDE		ARC-AMPE	
Mobile devices are excluded from the password complexity requirement.		characters, and at least one (1) each of uppercase letters, lowercase letters, numbers, and special characters.	
Control	**PKI-Based Authentication**	**Control**	**N/A**
IA-5 (2): PKI-Based Authentication For PKI-based authentication, the information system: **a.** Validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information; **b.** Enforces authorized access to the corresponding private key; **c.** Maps the authenticated identity to the account of the individual or group; and **d.** Implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.		**Withdrawn control**: No longer required for the minimum baseline but should still be considered best practice.	
Control	**In-Person or Trusted Third-Party Registration**	**Control**	**N/A**
IA-5 (3): In-Person or Trusted Third-Party Registration The organization requires that the registration process to receive hardware administrative tokens and credentials used for two (2)-factor authentication be conducted in person before a designated registration authority with authorization by defined personnel or roles (defined in the applicable security plan).		**Withdrawn control**: Incorporated into **IA-12(04)**.	
Control	**N/A**	**Control**	**Protection of Authenticators**
Existing NIST SP 800-53 Rev.4 control and new to ARC-AMPE.		**IA-05(06): Protection of Authenticators** Protect authenticators commensurate with the security category of the information to which use of the authenticator permits access.	
Control	**No Embedded Unencrypted Static Authenticators**	**Control**	**Authenticator Management | No Embedded Unencrypted Static Authenticators**
IA-5 (7): No Embedded Unencrypted Static Authenticators The organization ensures that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys.		**IA-05(07): Authenticator Management | No Embedded Unencrypted Static Authenticators** Ensure that unencrypted static authenticators are not embedded in applications or other forms of static storage.	
Control	**Hardware Token-Based Authentication**	**Control**	**N/A**
IA-5 (11): Hardware Token-Based Authentication The information system, for hardware token-based authentication, employs mechanisms that satisfy minimum token requirements.		**Withdrawn control**: Incorporated into **IA-02(01)** and **IA-02(02)**.	
Control	**Authenticator Feedback**	**Control**	**Authenticator Feedback**
IA-6: Authenticator Feedback The information system obscures feedback of authentication information during the authentication process to protect the		**IA-06: Authenticator Feedback**	

EDE		ARC-AMPE	
information from possible exploitation/use by unauthorized individuals.		Obscure feedback of authentication information during the authentication process to protect the information from possible exploitation and use by unauthorized individuals.	
Control	**Cryptographic Module Authentication**	**Control**	**Cryptographic Module Authentication**
IA-7: Cryptographic Module Authentication The information system implements mechanisms for authentication to a cryptographic module that meets the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.		**IA-07: Cryptographic Module Authentication** Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.	
Control	**Identification and Authentication (Non-Organizational Users)**	**Control**	**Identification and Authentication (Non-Organizational Users)**
IA-8: Identification and Authentication (Non-Organizational Users) The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users) prior to gaining access to all organizational systems and networks.		**IA-08: Identification and Authentication (Non-Organizational Users)** Uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users.	
Control	**Acceptance of Third-Party Credentials**	**Control**	**Identification and Authentication (Non-Organizational Users) |Acceptance of External Party Credentials**
IA-8 (2): Acceptance of Third-Party Credentials The information system accepts only FICAM-approved third-party credentials.		**IA-08(02): Identification and Authentication (Non-Organizational Users) |Acceptance of External Party Credentials** **a.** Accept only external authenticators that are NIST compliant; and **b.** Document and maintain a list of accepted external authenticators.	
Control	**N/A**	**Control**	**Re-Authentication**
Existing NIST SP 800-53 Rev.4 control and new to ARC-AMPE.		**IA-11: Re-Authentication** Require users to re-authenticate when organization-defined circumstances or situations occur requiring re-authentication.	
Control	**N/A**	**Control**	**Identity Proofing**
New NIST SP 800-53 Rev. 5 Control and applicable to ARC-AMPE		**IA-12: Identity Proofing** **c.** Identity proof users who require accounts for logical access to systems based on appropriate identity assurance level requirements as specified in applicable standards and guidelines; **d.** Resolve user identities to a unique individual; and **e.** Collect, validate, and verify identity evidence.	
Control	**N/A**	**Control**	**Supervisor Authorization**
New NIST SP 800-53 Rev. 5 Control and applicable to ARC-AMPE		**IA-12(01): Supervisor Authorization** Require that the registration process to receive an account for logical access includes supervisor or sponsor authorization.	

EDE		ARC-AMPE	
Control	**N/A**	**Control**	**Identity Evidence Validation and Verification**
New NIST SP 800-53 Rev. 5 Control and applicable to ARC-AMPE		**IA-12(03): Identity Evidence Validation and Verification** Require that the presented identity evidence be validated and verified through organization-approved methods of validation and verification..	

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 (Identification and Authentication (IA))_07142025