COALFIRE

WHITE PAPER

Migration from EDE to ARC-AMPE Contingency Planning (CP) 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 Contingency 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 (This Document)	**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.

Contingency Planning (CP)

The set of controls in this family focus on how the Exchange shall establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for Exchange IT systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

<table>
<tr><th colspan="2">EDE</th><th colspan="2">ARC-AMPE</th></tr>
<tr><td>Control</td><td>Contingency Planning Policy and Procedures</td><td>Control</td><td>Policy and Procedures</td></tr>
<tr><td colspan="2">CP-1: Contingency Planning Policy and Procedures
The organization:
a. Develops, documents, and disseminates to applicable personnel:
1. A contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.
b. Reviews and updates (as necessary) the current:
3. Contingency planning policy at least every three (3) years or as necessitated by significant change.
4. Contingency planning procedures at least every three (3) years or as necessitated by significant change.</td><td colspan="2">CP-01: Policy and Procedures
a. Develop, document, and disseminate to applicable personnel and roles:
1. Organization-level contingency planning 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 contingency planning policy and the associated contingency planning controls;
b. Designate an organization-defined official to manage the development, documentation, and dissemination of the contingency planning policy and procedures; and
c. Review and update the current contingency planning:
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.</td></tr>
<tr><td>Control</td><td>Contingency Plan</td><td>Control</td><td>Contingency Plan</td></tr>
<tr><td colspan="2">CP-2: Contingency Plan
The organization:
a. Develops a contingency plan for the information system in accordance with NIST SP 800-34 that:
1. Identifies essential organizational missions and business functions and associated contingency requirements;
2. Provides recovery objectives, restoration priorities, and metrics;
3. Addresses contingency roles, responsibilities, and assigns these to specific individuals with contact information;
4. Addresses maintaining essential organizational missions and business functions despite an information system disruption, compromise, or failure;
5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and
6. Is reviewed and approved by designated officials within the organization.
b. Distributes copies of the contingency plan to the Information System Security Officer, Business Owner,</td><td colspan="2">CP-02: Contingency Plan
a. Develop a contingency plan for the system that:
1. Identifies essential missions and business functions and associated contingency requirements;
2. Provides recovery objectives, restoration priorities, and metrics;
3. Addresses contingency roles, responsibilities, and assigned individuals with contact information;
4. Addresses maintaining essential missions and business functions despite a system disruption, compromise, or failure;
5. Addresses eventual, full system restoration without deterioration of the controls originally planned and implemented;
6. Addresses the sharing of contingency information; and
7. Is reviewed and approved by organization-defined personnel or roles (e.g., Contingency Plan Coordinator [CPC) and business owners);
b. Distribute copies of the contingency plan to organization-defined key contingency personnel or roles;
c. Coordinate contingency planning activities with incident handling activities;</td></tr>
</table>

<table>
<tr><th colspan="2">EDE</th><th colspan="2">ARC-AMPE</th></tr>
<tr><td colspan="2">Contingency Plan Coordinator, and other stakeholders identified within the contingency plan;
c. Coordinates contingency planning activities with incident-handling activities;
d. Reviews the contingency plan for the information system within every three hundred sixty-five (365) days;
e. Updates the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;
f. Communicates contingency plan changes to key contingency personnel system administrator, database administrator, and other personnel/roles as appropriate and organizational elements identified above; and
g. Protects the contingency plan from unauthorized disclosure and modification.

Implementation Standards
1. The system must be continuously monitored and assessed to ensure that it is operating as intended and that changes do not have an adverse effect on system performance.
2. The organization must verify that the provisioned implementation that is assessed and/or monitored meets users' needs and is an approved system configuration.
3. The organization defines a list of key contingency personnel (identified by name and/or by role) and organizational elements to whom the organization will distribute the CP.
4. The organization defines a list of key contingency personnel (identified by name and/or by role) and organizational elements to whom the organization will distribute the CP and communicate any changes.</td><td colspan="2">d. Review the contingency plan for the system within at least one (1) year;
e. Update the contingency plan to address changes to the organization, system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;
f. Communicate contingency plan changes to organization-defined key contingency personnel or roles;
g. Incorporate lessons learned from contingency plan testing, training, or actual contingency activities into contingency testing and training; and
h. Protect the contingency plan from unauthorized disclosure and modification.</td></tr>
<tr><td>Control</td><td>Coordinate with Related Plans</td><td>Control</td><td>Coordinate with Related Plans</td></tr>
<tr><td colspan="2">CP-2 (1): Coordinate with Related Plans
The organization coordinates contingency plan development with organizational elements responsible for related plans.</td><td colspan="2">CP-02(01): Coordinate with Related Plans
Coordinate contingency plan development with organizational elements responsible for related plans.</td></tr>
<tr><td>Control</td><td>Capacity Planning</td><td>Control</td><td>N/A</td></tr>
<tr><td colspan="2">CP-2 (2): Capacity Planning
The organization conducts capacity planning to ensure the necessary capacity for information processing, telecommunications, and environmental support during contingency operations.</td><td colspan="2">Withdrawn Control: No longer required for the minimum baseline but should still be considered a best practice.</td></tr>
<tr><td>Control</td><td>Resume Essential Missions/Business Functions</td><td>Control</td><td>Resume Missions and Business Functions</td></tr>
<tr><td colspan="2">CP-2 (3): Resume Essential Missions/Business Functions
The organization plans for the resumption of essential missions and business functions within the approved Maximum Tolerable Downtime (MTD), determined by the business owner, for the business functions.</td><td colspan="2">CP-02(03): Resume Missions and Business Functions
Plan for the resumption of essential mission and business functions within the Business Owner-approved Maximum Tolerable Downtime (MTD) of contingency plan activation.</td></tr>
</table>

EDE		ARC-AMPE	
Control	**Identify Critical Assets**	**Control**	**Identify Critical Assets**
CP-2 (8): Identify Critical Assets The organization identifies critical information system assets supporting essential missions and business functions.		**CP-02(08): Identify Critical Assets** Identify critical system assets supporting essential mission and business functions.	
Control	**Contingency Training**	**Control**	**Contingency Training**
CP-3: Contingency Training The organization provides contingency training to operational and support personnel (including managers and information system users) consistent with assigned roles and responsibilities: **a.** Within ninety (90) days of assuming a contingency role or responsibility; **b.** When required by information system changes; and **c.** Within every three hundred sixty-five (365) days thereafter.		**CP-03: Contingency Training** **a.** Provide contingency training to system users consistent with assigned roles and responsibilities: **1.** Within thirty (30) days of assuming a contingency role or responsibility; **2.** When required by system changes; and **3.** Every one (1) year thereafter; and **b.** Review and update contingency training content at least every one (1) year and following organization-defined events.	
Control	**Contingency Plan Testing**	**Control**	**Contingency Plan Testing**
CP-4: Contingency Plan Testing The organization: **a.** Tests the contingency plan for the information system within every three hundred sixty-five (365) days using NIST or organization-defined tests and exercises, such as tabletop tests, in accordance with the current organization contingency plan procedure to determine the effectiveness of the plan and the organizational readiness to execute the plan; **b.** Reviews the contingency plan test results; and **c.** Initiates corrective actions, if needed. **Implementation Standards** **1.** Must produce an after-action report to improve existing processes, procedures, and policies. **2.** Contingency plan test results will be made available to the organization business owner and all system developers and maintainers.		**CP-04: Contingency Plan Testing** **a.** Test the contingency plan for the system at least within every one (1) year using the following tests to determine the effectiveness of the plan and the readiness to execute the plan: the most current NIST SP 800-34, NIST SP 800-84, and any organization-defined functional tests or exercises; **b.** Review the contingency plan test results; and **c.** Initiate corrective actions, if needed.	
Control	**Coordinate with Related Plans**	**Control**	**Coordinate with Related Plans**
CP-4 (1): Coordinate with Related Plans The organization coordinates contingency plan testing with organizational elements responsible for related plans. **Implementation Standards** Organizations require a suite of plans to prepare themselves for response, continuity, recovery, and resumption of mission/business processes and information systems in the event of a disruption. Each plan has a specific purpose and scope: 1. Continuity of Operations Plan (COOP) 2. Business Continuity Plan (BCP) 3. Critical Infrastructure Protection (CIP) Plan		**CP-04(01): Coordinate with Related Plans** Coordinate contingency plan testing with organizational elements responsible for related plans.	

EDE		ARC-AMPE	
4. Disaster Recovery Plan (DRP) 5. Information System Contingency Plan (ISCP) 6. Cyber Incident Response Plan 7. Occupant Emergency Plan (OEP)			
Control	**Alternate Storage Site**	**Control**	**Alternate Storage Site**
CP-6: Alternate Storage Site The organization: **a.** Establishes an alternate storage site as well as the necessary agreements to permit the storage and retrieval of information system backup information; and **b.** Ensures that the alternate storage site provides information security safeguards equivalent to that of the primary site.		**CP-06: Alternate Storage Site** **a.** Establish an alternate storage site, including necessary agreements to permit the storage and retrieval of system backup information; and **b.** Ensure that the alternate storage site provides controls equivalent to that of the primary site.	
Control	**Separation from Primary Site**	**Control**	**Separation from Primary Site**
CP-6 (1): Separation from Primary Site The organization identifies an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same threats.		**CP-06(01): Separation from Primary Site** Identify an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same threats.	
Control	**Accessibility**	**Control**	**Accessibility**
CP-6 (3): Accessibility The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.		**CP-06(03): Accessibility** Identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outline explicit mitigation actions.	
Control	**Telecommunications Services**	**Control**	**N/A**
CP-8: Telecommunications Services The organization establishes alternate telecommunications services as well as the necessary agreements to permit the resumption of information system operations for essential organizational missions and business functions within the resumption time period specified in Implementation Standard 1 when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites. **Implementation Standards** **1.** Ensure alternate telecommunications Service Level Agreements (SLA) are in place to permit resumption of system Recovery Time Objectives (RTO) and business function Maximum Tolerable Downtimes (MTD). **2.** The system owner defines a resumption time consistent with the RTOs and business impact analysis. The time period is approved and accepted by the business owner.		**Withdrawn Control: Incorporated into SC-07(04)**	
Control	**Priority of Service Provisions**	**Control**	**N/A**
CP-8 (1): Priority of Service Provisions The organization:		**Withdrawn Control:** No longer required for the minimum baseline but should still be considered a best practice.	

EDE		ARC-AMPE	
a. Develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives); and **b.** Requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness if the primary and/or alternate telecommunications services are provided by a common carrier.			
Control	**Single Points of Failure**	**Control**	**N/A**
CP-8 (2): Single Points of Failure The organization obtains alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.		**Withdrawn Control**: No longer required for the minimum baseline but should still be considered a best practice.	
Control	**Information System Backup**	**Control**	**System Backup**
CP-9: Information System Backup The organization: **a.** Conducts backups of user-level information contained in the information system in accordance with the frequency specified in Implementation Standard 1; **b.** Conducts backups of system-level information contained in the information system in accordance with the frequency specified in Implementation Standard 1; **c.** Conducts backups of information system documentation, including security-related documentation, other forms of data, and paper records, within the frequency defined in the applicable security plan, consistent with recovery time and recovery point objectives; and **d.** Protects the confidentiality, integrity, and availability of backup information at storage locations. **Implementation Standards** **1.** Perform full backups weekly to separate media. Perform incremental or differential backups daily to separate media. Backups to include user-level and system-level information (including system state information). Three (3) generations of backups (full as well as all related incremental or differential backups) are stored off site. Off-site and on-site backups must be logged with name, date, time and action. **2.** The organization determines how Information System Backup is going to be verified and the appropriate periodicity of the check. **3.** Backups must be compliant with requirements for protecting data at rest. (see SC-28). **4.** The organization maintains at least three (3) backup copies of user-level information, system-level information, and information system documentation including security information (at least one (1) of which is available online) or provides an equivalent alternative. **5.** Ensure that a current, retrievable, copy of Personally Identifiable Information (PII) is available before movement of servers.		**CP-09: System Backup** **a.** Conduct backups of user-level information contained in organization-defined system components consistent with: **1.** Daily Incremental backups and weekly full backups; **2.** Maintaining three (3) generations of backups, at least one (1) of which is available online (a full backup and all related incremental backups); **b.** Conduct backups of system-level information contained in the system consistent with: **1.** Daily incremental backups and weekly full backups; **2.** Maintaining three (3) generations of backups, at least one (1) of which is available online (a full backup and all related incremental backups); **c.** Conduct backups of system documentation, including security- and privacy-related documentation consistent with: **1.** Daily incremental backups and weekly full backups; **2.** Maintaining three (3) generations of backups, at least one (1) of which is available online (a full backup and all related incremental backups); and **d.** Protect the confidentiality, integrity, and availability of backup information.	

EDE		ARC-AMPE	
6. (Cloud environments) The system owner shall determine what elements of the cloud environment require the Information System Backup control. **7.** (Cloud environments) The system owner determines how Information System Backup will be verified and the appropriate periodicity of the check. **8.** Use the encryption methodology specified in SC-13 to encrypt personally identifiable information (PII) confidentiality impact level information in backups at the storage location.			
Control	**Testing for Reliability/Integrity**	**Control**	**Testing for Reliability and Integrity**
CP-9(1): Testing for Reliability/Integrity The organization tests backup information following each backup, at least every six months, to verify media reliability and information integrity.		**CP-09(01): Testing for Reliability and Integrity** Test backup information at least every six (6) months to verify media reliability and information integrity.	
Control	**N/A**	**Control**	**Cryptographic Protection**
New NIST SP 800-53 Rev. 5 Control and applicable to ARC-AMPE		**CP-09(08): Cryptographic Protection** Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of all backup files.	
Control	**Information System Recovery and Reconstitution**	**Control**	**System Recovery and Reconstitution**
CP-10: Information System Recovery and Reconstitution The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure. Recovery of the information system after a failure or other contingency shall be done in a trusted, secure, and verifiable manner. **Implementation Standards** Secure information system recovery and reconstitution includes, but is not limited to: **a.** Reset all system parameters (either default or organization-established); **b.** Reinstall patches; **c.** Reestablish configuration settings; **d.** Reinstall application and system software; and **e.** Fully test the system.		**CP-10: System Recovery and Reconstitution** Provide for the recovery and reconstitution of the system to a known state within organization-defined time period specified in the contingency plan, or COOP after a disruption, compromise, or failure.	
Control	**Transaction Recovery**	**Control**	**Transaction Recovery**
CP-10 (2): Transaction Recovery The information system implements transaction recovery for transaction-based systems.		**CP-10(02): Transaction Recovery** Implement transaction recovery for systems that are transaction based.	

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 (Contingency Planning (CP))_07142025