COALFIRE

WHITE PAPER

Migration from EDE to ARC-AMPE Incident Response (IR) 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 Incident Response 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 (This Document)	**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.

Incident Response (IR)

The set of controls in this family focus on how the Exchange shall: (1) establish an operational incident-handling capability for Exchange IT systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (2) track, document, and report incidents to appropriate Exchange officials and/or authorities.

<table>
<tr><th colspan="2">EDE</th><th colspan="2">ARC-AMPE</th></tr>
<tr><td>Control</td><td>Incident Response Policy and Procedures</td><td>Control</td><td>Policy and Procedures</td></tr>
<tr><td colspan="2">IR-1: Incident Response Policy and Procedures
The organization:
a. Develops, documents, and disseminates to applicable personnel:
1. An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the incident response policy and associated incident response controls that are consistent with CMS Incident and Breach Notification Procedures within the CMS Risk Management Handbook.
b. Reviews and updates (as necessary) the current:
1. Incident response policy within every three (3) years; and
2. Incident response procedures within every three (3) years.</td><td colspan="2">IR-01: Policy and Procedures
a. Develop, document, and disseminate to applicable personnel or roles:
1. Organization-level incident response 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 incident response policy and the associated incident response controls;
b. Designate an organization-defined official to manage the development, documentation, and dissemination of the incident response policy and procedures; and
c. Review and update the current incident response:
3. Policy at least every one (1) year and following organization-defined events; and
4. Procedures at least every one (1) year and following organization-defined events.</td></tr>
<tr><td>Control</td><td>Incident Response Training</td><td>Control</td><td>Incident Response Training</td></tr>
<tr><td colspan="2">IR-2: Incident Response Training
The organization provides incident response training consistent with assigned roles and responsibilities to information system users:
a. Within one (1) month of assuming an incident response role or responsibility;
b. When required by information system changes; and
c. Within every three hundred sixty-five (365) days thereafter.

Implementation Standards
Formally tracks personnel participating in incident response training.</td><td colspan="2">IR-02: Incident Response Training
a. Provide incident response training to system users consistent with assigned roles and responsibilities:
1. Within one (1) month of assuming an incident response role or responsibility or acquiring system access;
2. When required by system changes; and
3. Within one (1) year thereafter; and
b. Review and update incident response training content every one (1) year and following defined events/incidents.</td></tr>
<tr><td>Control</td><td>N/A</td><td>Control</td><td>Breach</td></tr>
<tr><td colspan="2">New NIST SP 800-53 Rev. 5 Control and applicable to ARC-AMPE</td><td colspan="2">IR-02(03): Breach
Provide incident response training on how to identify and respond to a breach, including the organization’s process for reporting a breach.</td></tr>
</table>

EDE		ARC-AMPE	
Control	**Incident Response Testing**	**Control**	**Incident Response Testing**
IR-3: Incident Response Testing The organization tests the incident response capability for the information system, reviews and analyzes the results, performs simulations, and documents the test results to determine the incident response effectiveness within every three hundred sixty-five (365) days using NIST SP 800-61. **Implementation Standards** **1.** Incident response capability tests must exercise (or simulate exercise of) all organizational response capabilities. The organization's documented response to an actual historic incident may be used as part of an incident response capability test, and any response capabilities that were not exercised as part of the previous actual incident response activities must be additionally exercised (or simulated) as part of the test. **2.** The organization defines tests and/or exercises in accordance with NIST SP 800-61 (as amended).		**IR-03: Incident Response Testing** Test the effectiveness of the incident response capability for the system within every one (1) year using the following tests: appropriate organization-defined tests to determine the incident response effectiveness, and document the results.	
Control	**Coordination with Related Plans**	**Control**	**Coordination with Related Plans**
IR-3 (2): Coordination with Related Plans The organization coordinates incident response testing with organizational elements responsible for related plans.		**IR-03(02): Coordination with Related Plans** Coordinate incident response testing with organizational elements responsible for related plans.	
Control	**Incident Handling**	**Control**	**Incident Handling**
IR-4: Incident Handling The organization: **a.** Implements an incident handling capability (i.e., system incident response plan) using the current NIST SP 800-61; **b.** Coordinates incident handling activities with contingency planning activities; and **c.** Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises and implements the resulting changes accordingly. **d.** Ensures that individuals conducting incident handling meet personnel security requirements commensurate with the criticality/sensitivity of the information being processed, stored, and transmitted by the information system. **Implementation Standards** **1.** Document relevant information related to a security incident per the current organization incident handling and breach notification procedures. **2.** Preserve evidence through technical means, including secured storage of evidence media and "write" protection of evidence media. Use sound forensics processes and utilities that support legal requirements. Determine and follow a chain of custody for forensic evidence.		**IR-04: Incident Handling** **a.** Implement an incident handling capability for incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery; **b.** Coordinate incident handling activities with contingency planning activities; **c.** Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly; and **d.** Ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization.	

<table>
<tr><th colspan="2">EDE</th><th colspan="2">ARC-AMPE</th></tr>
<tr><td colspan="2">3. Identify vulnerability exploited during a security incident. Implement security safeguards to reduce risk and vulnerability exploit exposure, including isolating or disconnecting systems.
4. Incident response activities, to include forensic malware analysis, is coordinated with the ISSO. Each organization's security operations center:
a. Is responsible for actions to reduce the risk that an information security and/or privacy incident will occur and to respond appropriately to each incident or breach; and
b. Maintains primary responsibility for incident detection, including internal security monitoring and analysis of network traffic and logs.
5. Contact information for individuals with incident handling responsibilities must be maintained in the system Incident Response Plan.
a. Changes must be documented in the system incident response plan within three (3) days of the change.</td><td colspan="2"></td></tr>
<tr><td>Control</td><td>Automated Incident Handling Processes</td><td>Control</td><td>N/A</td></tr>
<tr><td colspan="2">IR-4 (1): Automated Incident Handling Processes
The organization employs automated mechanisms to support the incident handling process.

Implementation Standards
1. Automated mechanisms support the exchange of incident handling information within the organization:
a. Information is provided in a format compliant with incident handling procedure;
b. Incident handling information sources include systems, appliances, devices, services, and applications (including databases).
c. Incident handling information sources that do not support the exchange of information must be documented in the applicable risk assessment and security plan; and
d. Organization directed incident handling information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request.
2. Raw audit records must be available in an unaltered format.</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>N/A</td><td>Control</td><td>Continuity of Operations</td></tr>
<tr><td colspan="2">Existing NIST SP 800-53 Rev.4 control and new to ARC-AMPE.</td><td colspan="2">IR-04(03): Continuity of Operations
Identify classes of incidents and take the following actions in response to those incidents to ensure continuation of organizational missions and business function:
- Graceful degradation;
- Information system shutdown;</td></tr>
</table>

EDE		ARC-AMPE	
		- Fall back to manual mode/alternative technology whereby the system operates differently; - Employing deceptive measures; - Alternate information flows; or - Operating in a mode that is reserved solely for when systems are under attack.	
Control	**N/A**	**Control**	**Insider Threats – Specific Capabilities**
Existing NIST SP 800-53 Rev.4 control and new to ARC-AMPE.		**IR-04(06)**: **Insider Threats – Specific Capabilities** Implement an incident handling capability for incidents involving insider threats.	
Control	**Incident Monitoring**	**Control**	**Incident Monitoring**
IR-5: Incident Monitoring The organization tracks and documents physical, information security, and privacy incidents. **Implementation Standards** **1.** The organization forwards information system security and privacy incident and breach information: In accordance with reporting requirements defined in applicable incident response plans; and **2.** Provides incident and breach information in format compliant with organizational defined continuous monitoring requirements.		**IR-05: Incident Monitoring** Track and document incidents.	
Control	**Incident Reporting**	**Control**	**Incident Reporting**
IR-6: Incident Reporting The organization: **a.** Requires personnel to report suspected incidents to the organizational incident response capability within the timeframe established in the current organization Incident Handling Procedure and **b.** Reports security incident information to designated authorities. **Implementation Standards** **1.** Identify the organization's designated security and privacy official(s), if applicable, and/or identify other personnel authorized to access PII and responsible for reporting and managing Incidents or Breaches to CMS; **2.** Provide details regarding the identification, response, recovery, and follow-up of Incidents and Breaches, which should include information regarding the potential need for CMS to immediately suspend or revoke access to the Hub for containment purposes; and **3.** Require reporting of any security and privacy Incident or Breach of PII to the CMS IT Service Desk by telephone at (410) 786-2580 or 1-800-562-1963 or via email notification at cms_it_service_desk@cms.hhs.gov within one hour after discovery of the Incident or Breach.		**IR-06: Incident Reporting** **c.** Require personnel to report suspected incidents to the organizational incident response capability within the timeframe established in the current organization Incident Handling Procedure; and **d.** Report incident information to the organization-defined authorities.	

EDE		ARC-AMPE	
Control	**Automated Reporting**	**Control**	**Automated Reporting**
IR-6 (1): Automated Reporting The organization employs automated mechanisms to assist in the reporting of security incidents.		**IR-06(01): Automated Reporting** Report incidents using organization-defined automated mechanisms.	
Control	**Incident Response Assistance**	**Control**	**Incident Response Assistance**
IR-7: Incident Response Assistance The organization provides an incident response support resource integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.		**IR-07: Incident Response Assistance** Provide an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the system for the handling and reporting of incidents.	
Control	**Automation Support for Availability of Information/Support**	**Control**	**Automation Support for Availability of Information and Support**
IR-7 (1): Automation Support for Availability of Information/Support The organization employs automated mechanisms to increase the availability of incident response-related information and support.		**IR-07(01): Automation Support for Availability of Information and Support** Increase the availability of incident response information and support using organization-defined automated mechanisms to the maximum extent possible.	
Control	**Coordination with External Providers**	**Control**	**N/A**
IR-7 (2): Coordination with External Providers The organization: **a.** Establishes a direct, cooperative relationship between its incident response capability and external providers of information system protection capability; and **b.** Identifies organizational incident response team members to the external providers.		**Withdrawn Control**: No longer required for the minimum baseline but should still be considered a best practice.	
Control	**Incident Response Plan**	**Control**	**Incident Response Plan**
IR-8: Incident Response Plan The organization: **a.** Develops an incident response plan that: **1.** Provides the organization with a roadmap for implementing its incident response capability; **2.** Describes the structure and organization of the incident response capability; **3.** Provides a high-level approach for how the incident response capability fits into the overall organization; **4.** Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; **5.** Defines reportable incidents; **6.** Provides metrics for measuring the incident response capability within the organization; **7.** Defines the resources and management support needed to effectively maintain and mature an incident response capability; **8.** Is reviewed and approved by the applicable Incident Response Team Leader;		**IR-08: Incident Response Plan** **a.** Develop an Incident Response Plan that: **1.** Provides the organization with a roadmap for implementing its incident response capability; **2.** Describes the structure and organization of the incident response capability; **3.** Provides a high-level approach for how the incident response capability fits into the overall organization; **4.** Meets the unique requirements of the organization relating to mission, size, structure, and functions; **5.** Defines reportable incidents; **6.** Provides metrics for measuring the incident response capability within the organization; **7.** Defines the resources and management support needed to effectively maintain and mature an incident response capability; **8.** Addresses the sharing of incident information; **9.** Is reviewed and approved by the applicable Information System Security Officer (ISSO) and	

<table>
<tr><th colspan="2">EDE</th><th colspan="2">ARC-AMPE</th></tr>
<tr><td colspan="2">Distributes copies of the incident response plan to:
1. Chief Information Security Officer;
2. Chief Information Officer;
3. Information System Security Officer;
4. Office of the Inspector General/Computer Crimes Unit;
5. All personnel within the organization Incident Response Team;
6. All personnel within the PII Breach Response Team; and
7. All personnel within the organization Operations Centers.
c. Reviews within every three hundred sixty-five (365) days;
d. Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing;
e. Communicates incident response plan changes to the organizational elements listed in b. above; and
f. Protects the incident response plan from unauthorized disclosure and modification.</td><td colspan="2">approved by the Business Owner, at least every one (1) year; and
10. Explicitly designates responsibility for incident response to the applicable Information System Security Officer (ISSO), approved by the Business Owner.
b. Distribute copies of the Incident Response Plan to all personnel with a role or responsibility for implementing the Incident Response Plan;
c. Update the Incident Response Plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing;
d. Communicate Incident Response Plan changes to all personnel with a role or responsibility for implementing the Incident Response Plan; and
e. Protect the Incident Response Plan from unauthorized disclosure and modification.</td></tr>
<tr><td>Control</td><td>Information Spillage Response</td><td>Control</td><td>N/A</td></tr>
<tr><td colspan="2">IR-9: Information Spillage Response
The organization responds to information spills by:
a. a. Identifying the specific information involved in the information system contamination;
b. Alerting incident response personnel (as defined in the applicable security plan and the incident response plan [See IR-6]) of the information spill using a method of communication not associated with the spill;
c. Isolating the contaminated information system or system component;
d. Eradicating the information from the contaminated information system or component;
e. Identifying other information systems or system components that may have been subsequently contaminated; and
f. Performing required response actions as in the system incident response plan.</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>N/A</td><td>Control</td><td>Breaches</td></tr>
<tr><td colspan="2">New NIST SP 800-53 Rev. 5 Control and applicable to ARC-AMPE</td><td colspan="2">IR-08(01): Breaches
Include the following in the Incident Response Plan for breaches involving Personally Identifiable Information (PII):
(a) A process to determine if notice to individuals or other organizations, including oversight organizations, is needed;
(b) An assessment process to determine the extent of the harm, embarrassment, inconvenience, or unfairness to affected individuals and any mechanisms to mitigate such harms; and
(c) Identification of applicable privacy requirements.</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 (Incident Response (IR) _07142025