COALFIRE

WHITE PAPER

Migration from MARS-E to ARC-AMPE Incident Response (IR) controls

CMS requirements for Administering Entities

JESSICA PAYNE, CONSULTANT
IAN WALTERS, PRINCIPAL

877-224-8077 | info@coalfire.com | Coalfire.com

Table of contents

Purpose **2**
Background **3**
Affordable Care Act 3
CMS oversight 3
ARC-AMPE 3
Control mapping **4**
Incident Response (IR) 4
References **11**
Legal disclaimer **12**

Purpose

This white paper provides a guide for Administering Entities (AEs) to upgrade their System Security and Privacy Plans (SSPPs) from the Minimum Acceptable Risk Standards for Exchanges (MARS-E) 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	51
Awareness and Training	9
Audit and Accountability	19
Assessment, Authorization, and Monitoring	12
Configuration Management	31
Contingency Planning	23
Identification and Authentication	24
Incident Response (This Document)	**16**
Maintenance	16
Media Protection	9
Physical and Environmental Protection	19
Planning	6
Program Management	28
Personnel Security	9
Personally Identifiable Information Processing and Transparency	10
Risk Assessment	12
System and Services Acquisition	34
System and Communications Protection	34
System and Information Integrity	34
Supply Chain Risk Management	6

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.

CMS oversight

The Centers for Medicare & Medicaid Services (CMS) exercises oversight of AEs, 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 AEs to undergo rigorous audit processes, including demonstrating compliance with security and privacy control requirements.
- Enforcing strict data protection measures in the AE 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 AEs to adhere to operational policies and procedures, such as providing accurate plan information, maintaining transparent consumer interactions, and facilitating HIM enrollment without bias.
- Requiring AEs 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 AEs to renew their Authority to Connect (ATC) or Authority to Operate (ATO) annually, providing updated documentation and evidence of continued compliance with all requirements.

Through these oversight mechanisms, CMS ensures that AEs 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 Version 1.02 on April 9, 2025. This framework is slated to replace the Minimum Acceptable Risk Standards for Exchange (MARS-E) 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 ACA AEs.
- AEs must have ARC-AMPE implemented by March 4, 2026.
- The implementation date for EDE entities has yet to be announced as of the date of this white paper.

The minimum control baseline for ARC-AMPE compliance consists of 402 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 represents a significant increase from the MARS-E baseline, and AEs should be prepared for an increased level of effort for developing the SSPP and to submit more artifacts during audits.

Another major change is the format of the SSPP template. MARS-E uses a Microsoft Word format whereas ARC-AMPE is an Excel spreadsheet.

Control mapping

The mapping of the controls found in MARS-E Version 2.2 (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 MARS-E 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 MARS-E 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.

MARS-E		ARC-AMPE	
Control	**Incident Response Policy and Procedures**	**Control**	**Policy and Procedures**
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. **b.** Reviews and updates (as necessary) the current: **1.** Incident response policy within every three hundred sixty-five (365) days; and **2.** Incident response procedures within every three hundred sixty-five (365) days. Applicable personnel (item a) include the Incident Response Team as required by OMB M-17-12.		**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.	
Control	**Incident Response Training**	**Control**	**Incident Response Training**
IR-2: Incident Response Training The organization provides incident response training consistent with assigned roles and responsibilities to information system users:		**IR-02: Incident Response Training** **a.** Provide incident response training to system users consistent with assigned roles and responsibilities:	

MARS-E		ARC-AMPE	
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.		**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.	
Control	**N/A**	**Control**	**Breach**
New NIST SP 800-53 Rev.5 control and applicable to ARC-AMPE.		**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.	
Control	**Incident Response Testing**	**Control**	**Incident Response Testing**
IR-3: Incident Response Testing The organization tests the incident response capability for the information system within every three hundred sixty-five (365) days using NIST SP 800-61, reviews, analyses, and simulations to determine the organization's incident response effectiveness, and documents its findings. **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.** In a cloud environment, the service provider defines tests and/or exercises in accordance with NIST SP 800-61 (as amended). The service provider submits test plans to the Authorizing Official (AO) annually. Test plans are approved and accepted by the AO before the test begins.		**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 organizational Administering Entity Security and Privacy Incident Response Guidance; **b.** Coordinates incident handling activities with contingency planning activities;		**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,	

<table>
<tr><th colspan="2">MARS-E</th><th colspan="2">ARC-AMPE</th></tr>
<tr><td colspan="2">c. Incorporates lessons learned from ongoing incident-handling activities into incident response procedures, training, and testing/exercises and implements the resulting changes accordingly.

Implementation Standards
1. Document relevant information related to a security incident per the current organization and follow the Administering Entity Security and Privacy Incident Response Guidance, which can be found at: https://zone.cms.gov/document/aca-administering-entity-ae-incident-response-ir.
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.
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.
6. The organization 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.</td><td colspan="2">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.</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.</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;
• Fall back to manual mode/alternative technology whereby the system operates differently;</td></tr>
</table>

MARS-E		ARC-AMPE	
		• 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 to CMS 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 a format compliant with organizationally 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 ACA incident handling process available at: https://zone.cms.gov/community/cms-aca-program-security-privacy-policy-guidance-templates and **b.** Reports suspected security incident information to designated organizational authorities, which should be consistent with incident reporting timelines as specified in NIST SP 800-61 (as amended).		**IR-06: Incident Reporting** **a.** Require personnel to report suspected incidents to the organizational incident response capability within the timeframe established in the current organization Incident Handling Procedure; and **b.** Report incident information to the organization-defined authorities.	
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.	

MARS-E		ARC-AMPE	
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**	**Coordination with External Providers**
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.		**IR-07(02): Coordination with External Providers** **a.** Establish a direct, cooperative relationship between the organization's incident response capability and external providers of system protection capability; and **b.** Identify organizational incident response team members to the external providers.	
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; **9.** Is distributed to identified incident response personnel and organizational units, which may include: i. Chief Information Security Officer; ii. Chief Information Officer; iii. Information System Security Officer; iv. Attorney General/Computer Crimes Unit; v. Personnel within the organizations Incident Response Team; vi. Personnel within the Personally Identifiable Information (PII) Breach Response Team; and **b.** Reviews within every three hundred sixty-five (365) days; **c.** Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing;		**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 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.	

MARS-E	ARC-AMPE
d. Communicates incident response plan changes to the organizational elements listed in a.9 above; and **e.** Protects the incident response plan from unauthorized disclosure and modification. **Implementation Standards** **1.** The organization defines a list of incident response personnel (identified by name and/or by role) and organizational elements for distribution of the response plan. The incident response list includes designated CMS personnel. **2.** The organization defines a list of incident response personnel (identified by name and/or by role) and organizational elements for communication of any changes. The incident response list includes designated CMS personnel. **3.** Follow CMS guidance for Incident Handling, which can be found at: https://zone.cms.gov/community/cms-aca-program-security-privacy-policy-guidance-templates	
Control **N/A**	**Control** **Breaches**
New NIST SP 800-53 Rev.5 control and applicable to ARC-AMPE.	**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.
Control **Information Spillage Response**	**Control** **N/A**
IR-9: Information Spillage Response The organization responds to information spills by: **a.** Identifying the specific information involved in the improper or potentially improper information disclosure; **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.** Identifying other information systems or system components on which the information may have been subsequently improperly or potentially improperly shared with or disclosed to; and **e.** Removing and destroying the information from the contaminated information system, component or individual not authorized to handle the information. **f.** Requiring personnel to report suspected incidents to the organizational incident response capability within the timeframe established in the organizations Incident Handling Procedure and incident handling reporting process available at:	**Withdrawn Control**: No longer required for the minimum baseline but should still be considered a best practice.

MARS-E		ARC-AMPE	
https://zone.cms.gov/community/cms-aca-program-security-privacy-policy-guidance-templates			
Control	**Responsible Personnel**	**Control**	**N/A**
IR-9 (1): Responsible Personnel (Required for Cloud Environment; Recommended for Non-Cloud Environments) The organization assigns responsibility for responding to information spills to defined personnel or roles.		**Withdrawn Control**: No longer required for the minimum baseline but should still be considered a best practice.	
Control	**Training**	**Control**	**N/A**
IR-9 (2): Training The organization provides information spillage response training no less often than annually.		**Withdrawn Control**: No longer required for the minimum baseline but should still be considered a best practice.	
Control	**Post-Spill Operations**	**Control**	**N/A**
IR-9 (3): Post-Spill Operations (Required for Cloud Environment; Recommended for Non-Cloud Environments) The organization implements processes and procedures to ensure that organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions.		**Withdrawn Control**: No longer required for the minimum baseline but should still be considered a best practice.	
Control	**Exposure to Unauthorized Personnel**	**Control**	**N/A**
IR-9 (4): Exposure to Unauthorized Personnel The organization employs rules of behavior and defined security and privacy safeguards to address the risk of personnel exposed to information not within assigned access authorizations.		**Withdrawn Control**: No longer required for the minimum baseline but should still be considered a best practice.	

References

NIST SP 800-53 Revision 5.1.1

NIST SP 800-53 Revision 4

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**.

Copyright © 2025 Coalfire. All rights reserved. The information in this document is subject to change at any time based on revisions to applicable regulations and standards. Any forward-looking statements are not predictions and are subject to change without notice. Coalfire is not responsible for any errors or omissions.

WP_ACA CMS Controls Migration (Incident Response (IR) _03102025