COALFIRE

WHITE PAPER

Migration from MARS-E to ARC-AMPE Physical and Environmental Protection (PE) 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**
Physical and Environmental Protection (PE) 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 Physical and Environmental Protection 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	16
Maintenance	16
Media Protection	9
Physical and Environmental Protection (This Document)	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.

Physical and Environmental Protection (PE)

The set of controls in this family focus on how the exchange shall: (1) limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (2) protect the physical plant and support infrastructure for information systems; (3) provide supporting utilities for information systems; (4) protect information systems against environmental hazards; and (5) provide appropriate environmental controls in facilities containing information systems.

MARS-E		ARC-AMPE	
Control	**Physical and Environmental Protection Policy and Procedures**	**Control**	**Policy and Procedures**
PE-1: Physical and Environmental Protection Policy and Procedures The organization: **a.** Develops, documents, and disseminates to applicable personnel: **1.** A physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and **2.** Procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls. **b.** Reviews and updates (as necessary) the current: **1.** Physical and environmental protection policy within every three hundred sixty-five (365) days; and **2.** Physical and environmental protection procedures within every three hundred sixty-five (365) days.		**PE-01: Policy and Procedures** **a.** Develop, document, and disseminate to applicable personnel or roles: **1.** Organization-level physical and environmental protection 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 physical and environmental protection policy and the associated physical and environmental protection controls; **b.** Designate an organization-defined official to manage the development, documentation, and dissemination of the physical and environmental protection policy and procedures; and **c.** Review and update the current physical and environmental protection: **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.	

MARS-E		ARC-AMPE	
Control	**Physical Access Authorizations**	**Control**	**Physical Access Authorizations**
PE-2: Physical Access Authorizations The organization: **a.** Develops and maintains a current list of individuals with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible); **b.** Issues authorization credentials; and **c.** Reviews and approves the access list detailing authorization credentials every one hundred eighty (180) days, removing from the access list those personnel no longer requiring access. **d.** Removes individuals from the facility access list when access is no longer required. **Implementation Standards** **1.** Review and approve lists of personnel with authorized access to facilities containing information systems at least once every one hundred eighty (180) days. **2.** Create a restricted area, security room, or locked room to control access to areas containing Personally Identifiable Information (PII). These areas will be controlled accordingly.		**PE-02: Physical Access Authorizations** **a.** Develop, approve, and maintain a list of individuals with authorized access to the facility where the system resides; **b.** Issue authorization credentials for facility access; **c.** Review the access list detailing authorized facility access by individuals at least every six (6) months; and **d.** Remove individuals from the facility access list when access is no longer required.	
Control	**Access by Position / Role**	**Control**	**N/A**
PE-2(1): Access by Position / Role The organization authorizes physical access to the facility where the information system resides and information is received, processed, stored, or transmitted based on position or role.		**Withdrawn Control**: No longer required for the minimum baseline but should still be considered a best practice.	
Control	**Physical Access Control**	**Control**	**Physical Access Control**
PE-3: Physical Access Control The organization: **a.** Enforces physical access authorizations at defined entry/exit points to the facility (defined in the applicable security plan) where the information system resides by: **1.** Verifying individual access authorizations before granting access to the facility; and **2.** Controlling ingress/egress to the facility using guards and/or defined physical access control systems/devices (defined in the applicable security plan). **b.** Maintains physical access audit logs for defined entry/exit points (defined in the applicable security plan); **c.** Provides defined security safeguards (defined in the applicable security plan) to control access to areas within the facility officially designated as publicly accessible; **d.** Escorts visitors and monitors visitor activity in defined circumstances requiring visitor escorts and monitoring (defined in the applicable security plan); **e.** Secures keys, combinations, and other physical access devices;		**PE-03: Physical Access Control** **a.** Enforce physical access authorizations at entry and exit points to the facility where the system resides by: **1.** Verifying individual access authorizations before granting access to the facility; and **2.** Controlling ingress and egress to the facility using organization-defined physical access control systems or devices and/or guards; **b.** Maintain physical access audit logs for entry or exit points; **c.** Control access to areas within the facility designated as publicly accessible by implementing the following controls: organization-defined security safeguards or physical access controls; **d.** Escort visitors and control visitor activity in organization-defined circumstances requiring visitor escorts and controlling of visitor activity; **e.** Secure keys, combinations, and other physical access devices; **f.** Inventory organization-defined physical access devices every ninety (90) days; and **g.** Change combinations and keys at least every one (1) year or earlier as required by a security-relevant event	

MARS-E	ARC-AMPE
f. Inventories defined physical access devices (defined in the applicable security plan) no less often than every ninety (90) days; and **g.** Changes combinations and keys for defined high-risk entry/exit points (defined in the applicable security plan) within every three hundred sixty-five (365) days, and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated. **Implementation Standards** **1.** Control data center/facility access by use of door and window locks and security personnel or physical authentication devices, such as biometrics and/or smart card/PIN combination. **2.** Store and operate servers in physically secure environments and grant access to explicitly authorized personnel only. Access is monitored and recorded. **3.** Restrict access to grounds/facilities to authorized persons only. **4.** Store and operate servers in physically secure environments protected from unauthorized access. **5.** Create a restricted area, security room, or locked room to control access to areas containing PII. These areas will be controlled accordingly. **6.** Require two barriers to access PII under normal security: secured perimeter/locked container, locked perimeter/secured interior, or locked perimeter/security container. Protected information must be containerized in areas where other than authorized employees may have access afterhours.	and/or when keys are lost, combinations are compromised, or when individuals possessing the keys or combinations are transferred or terminated.
Control **Access Control for Transmission**	**Control** **Access Control for Transmission**
PE-4: Access Control for Transmission Medium The organization controls physical access to telephone closets and information system distribution and transmission lines within organizational facilities using defined security safeguards (defined in the applicable security plan). **Implementation Standards** Disable any physical ports (e.g., wiring closets and patch panels) not in use.	**PE-04: Access Control for Transmission** Control physical access to organization-defined system distribution and transmission lines within organizational facilities using organization-defined security controls or safeguards.
Control **Access Control for Output Devices**	**Control** **Access Control for Output Devices**
PE-5: Access Control for Output Devices The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.	**PE-05: Access Control for Output Devices** Control physical access to output from organization-defined output devices to prevent unauthorized individuals from obtaining the output.
Control **Monitoring Physical Access**	**Control** **Monitoring Physical Access**
PE-6: Monitoring Physical Access The organization: **a.** Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents;	**PE-06: Monitoring Physical Access** **a.** Monitor physical access to the facility where the system resides to detect and respond to physical security incidents;

MARS-E	ARC-AMPE
b. Reviews physical access logs weekly and upon occurrence of security incidents involving physical security; and **c.** Coordinates results of reviews and investigations with the organization's incident response capability	**b.** Review physical access logs at least monthly (every thirty [30] days) and upon occurrence of organization-defined events or potential indications of events; and **c.** Coordinate results of reviews and investigations with the organizational incident response capability.
Control **Intrusion Alarms/Surveillance Equipment**	**Control** **Intrusion Alarms and Surveillance Equipment**
PE-6 (1): Intrusion Alarms/Surveillance Equipment The organization monitors physical intrusion alarms and surveillance equipment.	**PE-06(01): Intrusion Alarms and Surveillance Equipment** Monitor physical access to the facility where the system resides using physical intrusion alarms and surveillance equipment.
Control **Visitor Access Records**	**Control** **Visitor Access Records**
PE-8: Visitor Access Records The organization: **a.** Maintains visitor access records to the facility where the information system resides for two (2) years; and **b.** Reviews visitor access records at least monthly. **Implementation Standards** At a minimum, visitor access records must include the following information: **1.** Name and organization of the person visiting; **2.** Visitor's signature; **3.** Form of identification; **4.** Date of access; **5.** Time of entry and departure; **6.** Purpose of visit; and **7.** Name and organization of person visited.	**PE-08: Visitor Access Records** **a.** Maintain visitor access records to the facility where the system resides for at least one (1) year; **b.** Review visitor access records at least monthly (every thirty [30] days); and **c.** Report anomalies in visitor access records to organization-defined personnel or roles.
Control **Power Equipment and Cabling**	**Control** **Power Equipment and Cabling**
PE-9: Power Equipment and Cabling The organization protects power equipment and power cabling for the information system from damage and destruction. **Implementation Standards** Permit only authorized maintenance personnel to access infrastructure assets, including power generators, HVAC systems, cabling, and wiring closets.	**PE-09: Power Equipment and Cabling** Protect power equipment and power cabling for the system from damage and destruction.
Control **Emergency Shutoff**	**Control** **Emergency Shutoff**
PE-10: Emergency Shutoff The organization: **a.** Provides the capability of shutting off power to the information system or individual system components in emergency situations; **b.** Places emergency shutoff switches or devices in a location that does not require personnel to approach the equipment to facilitate safe and easy access for personnel; and **c.** Protects emergency power shutoff capability from unauthorized activation.	**PE-10: Emergency Shutoff** **a.** Provide the capability of shutting off power to an organization-defined system or individual system components in emergency situations; **b.** Place emergency shutoff switches or devices in an organization-defined location by system or system component to facilitate access for authorized personnel; and **c.** Protect emergency power shutoff capability from unauthorized activation.

MARS-E		ARC-AMPE	
Implementation Standards Implements and maintains a master power switch or emergency cut-off switch, prominently marked and protected by a cover, for data centers, servers, and mainframe rooms.			
Control	**Emergency Power**	**Control**	**Emergency Power**
PE-11: Emergency Power The organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system and/or transition of the information system to a long-term alternate power source in the event of a primary power source loss.		**PE-11: Emergency Power** Provide an uninterruptible power supply to facilitate an orderly shutdown of the system and/or transition of the system to long-term alternate power in the event of a primary power source loss.	
Control	**Emergency Lighting**	**Control**	**Emergency Lighting**
PE-12: Emergency Lighting The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and covers emergency exits and evacuation routes within the facility. **Implementation Standards** Tests the equipment on a schedule that complies with manufacturer recommendations and local, state, and federal requirements. Testing must comply with the previously mentioned recommendations and be performed no less often than every three (3) years.		**PE-12: Emergency Lighting** Employ and maintain automatic emergency lighting for the system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.	
Control	**Fire Protection**	**Control**	**Fire Protection**
PE-13: Fire Protection The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source. **Implementation Standards** Tests the equipment on a schedule that complies with manufacturer recommendations and local, state, and federal requirements. Testing must comply with the previously mentioned recommendations and be performed no less often than every three (3) years.		**PE-13: Fire Protection** Employ and maintain fire detection and suppression systems that are supported by an independent energy source.	
Control	**N/A**	**Control**	**Detection Systems - Automatic Activation and Notification**
Existing NIST SP 800-53 Rev.4 control which was not selected for MARS-E version 2.2 and is applicable to ARC-AMPE.		**PE-13(01): Detection Systems - Automatic Activation and Notification** Employ fire detection systems that activate automatically and notify organization-defined personnel or roles and defined emergency responders in the event of a fire.	
Control	**Automatic Fire Suppression**	**Control**	**N/A**
PE-13 (3): Automatic Fire Suppression		**Withdrawn Control**: Incorporated into **PE-13(2)**.	

MARS-E		ARC-AMPE	
The organization employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.			
Control	**Temperature and Humidity Controls**	**Control**	**Environmental Controls**
PE-14: Temperature and Humidity Controls The organization: **a.** Maintains temperature and humidity levels within the facility where the information system resides within acceptable vendor-specified levels; **b.** Monitors temperature and humidity levels within the defined frequency (defined in the applicable security plan); and **c.** Tests the equipment on a schedule that complies with manufacturer recommendations and local, state, and federal requirements, no less often than three hundred sixty-five (365) days. **Implementation Standards** **1.** Evaluate the level of alert and follow prescribed guidelines for that alert level. **2.** Alert component management of possible loss of service and/or media. **3.** Report damage and provide remedial action. Implement contingency plan, if necessary. **4.** For Cloud Environment, the organization: **a.** Maintains temperature and humidity levels within the facility where the information system resides at levels consistent with American Society of Heating, Refrigerating and Air-conditioning Engineers (ASHRAE) document entitled “Thermal Guidelines for Data Processing Environments”; **b.** Monitors temperature and humidity levels continuously; and **c.** Measures temperature at server inlets and humidity levels by dew point.		**PE-14: Environmental Controls** **a.** Maintain temperature, humidity, and pressure levels at acceptable vendor-specified levels within the facility where the system resides; and **b.** Monitor environmental control levels within the defined frequency.	
Control	**Water Damage Protection**	**Control**	**Water Damage Protection**
PE-15: Water Damage Protection The organization protects the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel. **Implementation Standards** Tests the equipment on a schedule that complies with manufacturer recommendations and local, state, and federal requirements, no less often than three hundred sixty-five (365) days.		**PE-15: Water Damage Protection** Protect the system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.	
Control	**Delivery and Removal**	**Control**	**Delivery and Removal**
PE-16: Delivery and Removal The organization authorizes, monitors, and controls the flow of information system-related components entering and exiting the facility and maintains records of those items.		**PE-16: Delivery and Removal** **a.** Authorize and control all system components entering and exiting the facility; and **b.** Maintain records of the system components.	

<table>
<tr><th colspan="2">MARS-E</th><th colspan="2">ARC-AMPE</th></tr>
<tr><td>Control</td><td>Alternate Work Site</td><td>Control</td><td>Alternate Work Site</td></tr>
<tr><td colspan="2">PE-17: Alternate Work Site
The organization:
a. Employs appropriate security controls at alternate work sites that include, but are not to be limited to, requiring the use of laptop cable locks, recording serial numbers and other identification information about laptops;
b. Assesses, as feasible, the effectiveness of security controls at alternate work sites; and
c. Provides a means for employees to communicate with information security personnel in case of security incidents or problems.

Implementation Standards
The organization defines management, operational, and technical information system security controls for alternate work sites.</td><td colspan="2">PE-17: Alternate Work Site
a. Determine and document the alternate work sites allowed for use by employees;
b. Employ the following controls at alternate work sites: organization-defined controls;
c. Assess the effectiveness of controls at alternate work sites; and
d. Provide a means for employees to communicate with information security and privacy personnel in case of incidents.</td></tr>
<tr><td>Control</td><td>N/A</td><td>Control</td><td>Facility Location</td></tr>
<tr><td colspan="2">New NIST SP 800-53 Rev.5 Control and applicable to ARC-AMPE.</td><td colspan="2">PE-23: Facility Location
a. Plan the location or site of the facility where the system resides considering physical and environmental hazards; and
b. For existing facilities, consider the physical and environmental hazards in the organizational risk management strategy.</td></tr>
</table>

References

NIST SP 800-53 Revision 5.1.1

NIST SP 800-53 Revision 4

CMS Standards

Legal disclaimer

This white paper is provided by Coalfire Systems, Inc. or its subsidiaries (“Coalfire”) for informational purposes only. This white paper is the property of Coalfire and is protected by U.S. and international copyright laws. Unauthorized use, reproduction, or distribution of this white paper, in whole or in part, is strictly prohibited. Factual information included in this white paper has been taken from sources that Coalfire believes to be reliable, but its accuracy, completeness, or interpretation cannot be guaranteed. Information is current as of the date of this white paper only and is subject to change without notice. This white paper is provided “as-is” with no warranties, including any warranty of merchantability, fitness for a particular purpose, and non-infringement. Coalfire expressly disclaims all liability arising from or relating to the use of any information or material included in this white paper for any purpose, including any actions taken or not taken based on the contents of this white paper. You are solely responsible for making your own independent assessment of the information in this white paper and for the development, implementation, and execution of your information security program. For questions regarding any legal or compliance matters referenced in this white paper, you should consult your legal counsel, security advisor, or the relevant standard authority.

About the authors

Jessica Payne, Consultant

Jessica joined Coalfire in 2024 with five prior years of cybersecurity consulting experience. She supports our clients as a Consultant for the GRC Healthcare team where she specializes in cybersecurity risk management, cybersecurity program advisory, and compliance for the healthcare industry.

Her extensive experience in cybersecurity consulting allows her to provide customized solutions and guidance on industry best practices, greatly improving client security postures and ensuring compliance with regulatory standards. She is dedicated to ongoing improvement and to staying abreast of the latest cybersecurity trends and technologies to offer innovative solutions to her clients.

Ian Walters, Principal

Ian is a seasoned cybersecurity professional with a wealth of experience across a spectrum of frameworks and standards, including NIST SP 800-53, HIPAA, ISO 27001, ISO 20000, and ISO 9001.

With a meticulous eye for detail and a strategic mindset, Ian excels in developing tailored solutions to ensure compliance and mitigate risks within complex organizational environments. His expertise extends to leading audits and risk assessments, as well as providing advisory for driving continuous improvement initiatives to enhance cybersecurity posture and operational resilience.

About Coalfire

The world's leading technology infrastructure providers, SaaS companies, and enterprises – including the top 5 cloud service providers and 8 of the top 10 SaaS businesses – rely on Coalfire to strengthen their security posture and secure their digital transformations. As the largest firm dedicated to cybersecurity, Coalfire delivers a comprehensive suite of advisory and managed services, spanning cyber strategy and risk, cloud security, threat and vulnerability management, application security, privacy, and compliance management. A proven leader in cybersecurity for the past 20 years, Coalfire combines extensive cloud expertise, advanced technology, and innovative approaches that fuel success. For more information, visit **Coalfire.com**.

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 (Physical and Environmental Protection (PE))_03102025