COALFIRE

WHITE PAPER

Migration from MARS-E to ARC-AMPE Personally Identifiable Information Processing and Transparency (PT) 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**
Personally Identifiable Information Processing and Transparency (PT) 4
References **7**
Legal disclaimer **8**

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 whitepaper is one of a series of 20 which divides the ARC-AMPE by control family. This white paper addresses the Personally Identifiable Information Processing and Transparency 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	19
Planning	6
Program Management	28
Personnel Security	9
Personally Identifiable Information Processing and Transparency (This Document)	**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.

Personally Identifiable Information Processing and Transparency (PT)

This domain includes controls that govern the collection, use, processing, sharing, and disposal of Personally Identifiable Information (PII) while maintaining accountability, data accuracy, and user awareness. It emphasizes privacy risk management, consent mechanisms, data minimization, and ensuring individuals have visibility into how their data is used.

MARS-E		ARC-AMPE	
Control	**N/A**	**Control**	**Policy and Procedures**
New NIST SP 800-53 Rev.5 Control and applicable to ARC-AMPE.		**PT-01: Policy and Procedures** **a.** Develop, document, and disseminate to organization-defined personnel and roles: **1.** An organizational-level Personally Identifiable Information (PII) processing and transparency 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 PII processing and transparency policy and the associated PII processing and transparency controls; **b.** Designate an organization-defined official to manage the development, documentation, and dissemination of the PII processing and transparency policy and procedures; and **c.** Review and update the current PII processing and transparency: **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	**N/A**	**Control**	**Authority to Process Personally Identifiable Information**
• New NIST SP 800-53 Rev.5 Control and applicable to ARC-AMPE. • Withdrawn controls **AP-1** and **UL-2**.		**PT-02: Authority to Process Personally Identifiable Information** **a.** Determine and document the organization-defined authority that permits the organization-defined processing of Personally Identifiable Information (PII); and **b.** Restrict the organization-defined processing of PII to only that which is authorized.	
Control	**N/A**	**Control**	**Personally Identifiable Information Processing Purposes**
• New NIST SP 800-53 Rev.5 Control and applicable to ARC-AMPE. • Withdrawn controls **AP-2**, **UL-1**, and **UL-2**.		**PT-03: Personally Identifiable Information Processing Purposes** **a.** Identify and document the organization-defined purpose(s) for processing Personally Identifiable Information (PII); **b.** Describe the purpose(s) in the public privacy notices and policies of the organization; **c.** Restrict the organization-defined processing of PII to only that which is compatible with the identified purpose(s); and **d.** Monitor changes in processing PII and implement organization-defined mechanisms to ensure that any changes are made in accordance with organization-defined requirements.	
Control	**N/A**	**Control**	**Consent**
• New NIST SP 800-53 Rev.5 Control and applicable to ARC-AMPE • Withdrawn control **IP-1**.		**PT-04: Consent** Implement organization-defined tools or mechanisms for individuals to consent to the processing of their Personally Identifiable Information (PII) prior to its collection that facilitate individuals' informed decision-making.	
Control	**N/A**	**Control**	**Revocation**
New NIST SP 800-53 Rev.5 Control and applicable to ARC-AMPE.		**PT-04(03): Revocation** Implement organization-defined tools or mechanisms for individuals to revoke consent to the processing of their Personally Identifiable Information (PII).	
Control	**N/A**	**Control**	**Privacy Notice**
• New NIST SP 800-53 Rev.5 Control and applicable to ARC-AMPE. • Withdrawn controls **TR-1** and **IP-2**.		**PT-05: Privacy Notice** Provide notice to individuals about the processing of Personally Identifiable Information (PII) that: **a.** Is available to individuals upon first interacting with an organization, and subsequently at organization-defined frequency; **b.** Presents clear and easy to understand information about PII processing in plain language; **c.** Identifies the authority that authorizes the processing of PII; **d.** Identifies the purposes for which PII is to be processed; and	

<table>
<tr><th colspan="2">MARS-E</th><th colspan="2">ARC-AMPE</th></tr>
<tr><td colspan="2"></td><td colspan="2">e. Includes any additional information the organization deems necessary to effect compliance with applicable laws, regulations, or policies.</td></tr>
<tr><td>Control</td><td>N/A</td><td>Control</td><td>Just-in-time Notice</td></tr>
<tr><td colspan="2">New NIST SP 800-53 Rev.5 Control and applicable to ARC-AMPE.
Withdrawn control TR-1.</td><td colspan="2">PT-05(01): Just-in-time notice
Present notice of Personally Identifiable Information (PII) processing to individuals at a time and location where the individual provides PII or in conjunction with a data action, or at an organization-defined frequency.</td></tr>
<tr><td>Control</td><td>N/A</td><td>Control</td><td>Privacy Act Statements</td></tr>
<tr><td colspan="2">New NIST SP 800-53 Rev.5 Control and applicable to ARC-AMPE
Withdrawn control TR-2.</td><td colspan="2">PT-05(02): Privacy Act Statements
Include Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.</td></tr>
<tr><td>Control</td><td>N/A</td><td>Control</td><td>Specific Categories of Personally Identifiable Information</td></tr>
<tr><td colspan="2">New NIST SP 800-53 Rev.5 Control and applicable to ARC-AMPE.
Withdrawn controls IP-2 and TR-2.</td><td colspan="2">PT-07: Specific Categories of Personally Identifiable Information
Apply organization-defined processing conditions for specific categories of Personally Identifiable Information (PII).</td></tr>
<tr><td>Control</td><td>N/A</td><td>Control</td><td>Social Security Numbers</td></tr>
<tr><td colspan="2">New NIST SP 800-53 Rev.5 Control and applicable to ARC-AMPE.</td><td colspan="2">PT-07(01): Social Security Numbers
When a system processes Social Security numbers:
(a) Eliminate unnecessary collection, maintenance, and use of Social Security numbers, and explore alternatives to their use as a personal identifier;
(b) Do not deny any individual any right, benefit, or privilege provided by law because of such individual’s refusal to disclose his or her Social Security number; and
(c) Inform any individual who is asked to disclose his or her Social Security number whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it.</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 (Personally Identifiable Information Processing and Transparency (PT))_0310025