COALFIRE

WHITE PAPER

Migration from EDEE to ARC-AMPE Personally Identifiable Information Processing and Transparency (PT) 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 ..... Error! Bookmark not defined.
Background ..... Error! Bookmark not defined.
Affordable Care Act ..... **Error! Bookmark not defined.**
Enhanced Direct Enrollment ..... **Error! Bookmark not defined.**
CMS oversight ..... **Error! Bookmark not defined.**
ARC-AMPE ..... **Error! Bookmark not defined.**
Control mapping ..... Error! Bookmark not defined.
Personally Identifiable Information Processing and Transparency (PT) 5
References **8**
Legal disclaimer **9**

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 Personally Identifiable Information Processing and Transparency 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	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 (This Document)	**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.

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.

<table>
<tr><th colspan="2">EDE</th><th colspan="2">ARC-AMPE</th></tr>
<tr><td>Control</td><td>N/A</td><td>Control</td><td>Policy and Procedures</td></tr>
<tr><td colspan="2">New NIST SP 800-53 Rev.5 Control and applicable to ARC-AMPE.</td><td colspan="2">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.</td></tr>
<tr><td>Control</td><td>N/A</td><td>Control</td><td>Authority to Process Personally Identifiable Information</td></tr>
<tr><td colspan="2">• New NIST SP 800-53 Rev.5 Control and applicable to ARC-AMPE.
• Withdrawn controls AP-1 and UL-2.</td><td colspan="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.</td></tr>
<tr><td>Control</td><td>N/A</td><td>Control</td><td>Personally Identifiable Information Processing Purposes</td></tr>
<tr><td colspan="2">• New NIST SP 800-53 Rev.5 Control and applicable to ARC-AMPE.
• Withdrawn controls AP-2, UL-1, and UL-2.</td><td colspan="2">PT-03: Personally Identifiable Information Processing Purposes
a. Identify and document the organization-defined purpose(s) for processing Personally Identifiable Information (PII);</td></tr>
</table>

<table>
<tr><th colspan="2">EDE</th><th colspan="2">ARC-AMPE</th></tr>
<tr><td colspan="2"></td><td colspan="2">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.</td></tr>
<tr><td>Control</td><td>N/A</td><td>Control</td><td>Consent</td></tr>
<tr><td colspan="2">• New NIST SP 800-53 Rev.5 Control and applicable to ARC-AMPE
• Withdrawn control IP-1.</td><td colspan="2">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.</td></tr>
<tr><td>Control</td><td>N/A</td><td>Control</td><td>Revocation</td></tr>
<tr><td colspan="2">New NIST SP 800-53 Rev.5 Control and applicable to ARC-AMPE.</td><td colspan="2">PT-04(03): Revocation
Implement organization-defined tools or mechanisms for individuals to revoke consent to the processing of their Personally Identifiable Information (PII).</td></tr>
<tr><td>Control</td><td>N/A</td><td>Control</td><td>Privacy Notice</td></tr>
<tr><td colspan="2">• New NIST SP 800-53 Rev.5 Control and applicable to ARC-AMPE.
• Withdrawn controls TR-1 and IP-2.</td><td colspan="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
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</td></tr>
</table>

<table>
<tr><th colspan="2">EDE</th><th colspan="2">ARC-AMPE</th></tr>
<tr><td colspan="2"></td><td colspan="2">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

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 (Personally Identifiable Information Processing and Transparency (PT))_07142025