COALFIRE

WHITE PAPER

Migration from EDE to ARC-AMPE Access Control (AC) controls

CMS requirements for Direct Enrollment Entities

JESSICA PAYNE, CONSULTANT
IAN WALTERS, PRINCIPAL

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

Table of contents

Purpose

This white paper provides a guide for Direct Enrollment Entities (DEEs) to upgrade their Enhanced Direct Enrollment (EDE) System Security and Privacy Plans (SSPPs) to the Acceptable Risk Controls for ACA, Medicaid, and Provider Entities (ARC-AMPE).

Due to the substantial number of controls, and to facilitate ease of use, this white paper is one of a series of 20 which divides the ARC-AMPE by control family. This white paper addresses the Access Control controls.

ARC-AMPE Control Families	
Control Family	**Number of Controls**
Access Control (This Document)	**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	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.

Access Control (AC)

The controls listed in this section focus on how the Exchange shall limit IT system access to authorized users and devices, as well as processes acting on behalf of authorized users or devices and also describes the authorized transactions and functions that those users and devices are permitted to execute.

EDE		ARC-AMPE	
Control	**Access Control Policy and Procedures**	**Control**	**Policies and Procedures**
AC-1: Access Control Policy and Procedures The organization: a. Develops, documents, and disseminates to applicable personnel: 1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the access control policy and associated access controls; and b. Reviews and updates (as necessary) the current: 1. Access control policy at least every three (3) years; and 2. Access control procedures at least every three (3) years.		**AC-01: Policy and Procedures** a. Develop, document, and disseminate to applicable personnel and roles: 1. Organization-level access control 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 that are defined within the applicable control implementation statements of the associated access controls; b. Designate an organization-defined official to manage the development, documentation, and dissemination of the access control policy and procedures; and c. Review and update the current access control: 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.	
Control	**Account Management**	**Control**	**Account Management**
AC-2: Account Management The organization: a. Identifies and selects the following types of information system accounts (e.g., individual, group, system, application, guest/anonymous, emergency, and temporary) to support organizational missions/business functions; b. Assigns account managers for information system accounts; c. Establishes conditions for group and role membership;		**AC-02: Account Management** a. Define and document the type of accounts allowed and specifically prohibited for use within the system; b. Assign account managers; c. Require organization-defined prerequisites and criteria for group and role membership; d. Specify: 1. Authorized users of the system; 2. Group and role membership; and	

EDE	ARC-AMPE
d. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account; e. Requires approvals by defined personnel or roles (defined in the applicable security plan) for requests to create information system accounts; f. Creates, enables, modifies, disables, and removes information system accounts in accordance with the organization requirements, standards, and procedures; g. Monitors the use of information system accounts; h. Notifies account managers: 1. When accounts are no longer required; 2. When users are terminated or transferred; and 3. When individual information system usage or need-to-know changes; i. Authorizes access to the information system based on: 1. A valid access authorization; 2. Intended system usage; and 3. Other attributes as required by the organization or associated missions/business functions; j. Reviews accounts for compliance with account management requirements at least every ninety (90) days; and k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group. **Implementation Standards** 1. Remove or disable default user accounts. Rename active default accounts. 2. Implement centralized control of user access administrator functions. a. Regulate the access provided to contractors and define security requirements for contractors. b. Notify account managers within an organization-defined timeframe when temporary accounts are no longer required or when information system users are terminated or transferred or information system usage or need-to-know/need-to-share changes. 3. Prohibit use of guest, anonymous, and shared accounts for providing access to PII. 4. Notify account managers within an organization-defined timeframe when temporary accounts are no longer required or when IS users are terminated or transferred or IS usage or need-to-know/need-to-share changes. 5. Prior to granting access to PII, users demonstrate a need for the PII in the performance of the user's duties. 6. Implement access controls within the IS based on users' or user group's need for access to PII in the performance of their duties. 7. Organizations should provide access only to the minimum amount of PII necessary for users to perform their duties. 8. Create, enable, modify, disable, and remove information system accounts in accordance with the requirement for	3. Access authorizations (i.e., privileges) and organization-defined attributes (as required) for each account; e. Require approvals by organization-defined personnel or roles for requests to create accounts; f. Create, enable, modify, disable, and remove accounts in accordance with organization-defined policy, procedures, prerequisites, and criteria; g. Monitor the use of accounts; h. Notify account managers and organization-defined personnel or roles within: 1. Twenty-four (24) hours when accounts are no longer required; 2. Eight (8) hours when users are terminated or transferred; and 3. Eight (8) hours when system usage or need-to-know changes for an individual; i. Authorizes access to the system based on: 1. A valid access authorization; 2. Intended system usage; and 3. Other attributes as required by the organization or associated missions/business functions; j. Review accounts for compliance with account management requirements at least every ninety (90) days for all systems; and k. Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; and l. Align account management processes with personnel termination and transfer processes.

EDE		ARC-AMPE	
each user to complete privacy training every 365 days otherwise the account would be disabled.			
Control	**Automated Information System Account Management**	**Control**	**Automated System Account Management**
AC-2(1): Automated Information System Account Management The organization employs automated mechanisms to support the management of information system accounts.		**AC-02(01): Automated System Account Management** Support the management of system accounts using organization-defined automated mechanisms.	
Control	**Removal of Temporary/Emergency Accounts**	**Control**	**Automated Temporary and Emergency Account Management**
AC-2(2): Removal of Temporary/Emergency Accounts The information system automatically disables emergency accounts within twenty-four (24) hours and temporary accounts with a fixed duration not to exceed sixty (60) days.		**AC-02(02): Automated Temporary and Emergency Account Management** Automatically disable temporary and emergency accounts after no more than ninety-six (96) hours from last use.	
Control	**Disable Inactive Accounts**	**Control**	**Disable Accounts**
AC-2(3): Disable Inactive Accounts The information system automatically disables inactive accounts within sixty (60) days.		**AC-02(03): Disable Accounts** Disable non-consumer accounts within twenty-four (24) hours when the accounts: a. Have expired; b. Are no longer associated with a user or individual; c. Are in violation of organizational policy; or d. Have been inactive for sixty (60) days.	
Control	**Automated Audit Actions**	**Control**	**Automated Audit Actions**
AC-2(4): Automated Audit Actions The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies defined personnel or roles (defined in the applicable security plan). **Implementation Standards** Account management information sources include systems, appliances, devices, services, and applications (including databases).		**AC-02(04): Automated Audit Actions** Automatically audit system account creation, modification, enabling, disabling, and removal actions.	
Control	**N/A**	**Control**	**Inactivity Logout**
Existing NIST SP 800-53 Rev.4 control and new to ARC-AMPE.		**AC-02(05): Inactivity Logout** Require that users log out when the time-period of inactivity will exceed twenty-four (24) hours.	
Control	**Role-Based Schemes**	**Control**	**Privileged User Accounts**
AC-2(7): Role-Based Schemes The organization: a. Establishes and administers application-specific privileged user accounts in accordance with a role-based		**AC-02(07): Privileged User Accounts** a. Establish and administer privileged user accounts in accordance with a role-based access scheme; b. Monitor privileged role or attribute assignments;	

EDE		ARC-AMPE	
access scheme that allows access based on user responsibilities associated with application use; b. Monitors privileged role assignments as well as application-specific privileged role assignments; and c. Takes corrective actions when privileged role assignments are no longer appropriate.		c. Monitor changes to roles or attributes; and d. Revoke access when privileged role or attribute assignments are no longer appropriate.	
Control	**Shared/Group Account Credential Termination**	**Control**	**N/A**
AC-2 (10): Shared/Group Account Credential Termination The information system updates shared/group account credentials when members leave the group.		**Withdrawn Control**: Incorporated into **AC-02**.	
Control	**N/A**	**Control**	**Account Monitoring for Atypical Usage**
Existing NIST SP 800-53 Rev.4 control and new to ARC-AMPE.		**AC-02(12): Account Monitoring for Atypical Usage** a. Monitor system accounts for atypical use; and b. Report atypical usage of system accounts to organization-defined personnel or roles, and if necessary, any applicable incident response team(s).	
Control	**N/A**	**Control**	**Disable Accounts for High-Risk Individuals**
Existing NIST SP 800-53 Rev.4 control and new to ARC-AMPE.		**AC-02(13): Disable Accounts for High-Risk Individuals** Disable accounts of individuals within one (1) hour of discovery of individual posing as a significant risk.	
Control	**Access Enforcement**	**Control**	**Access Enforcement**
AC-3: Access Enforcement The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. **Implementation Standards** 1. If encryption is used as an access control mechanism, it must meet FIPS 140-2 compliant encryption standards (see SC 13). 2. Configure operating system controls to disable public "read" and "write" access to files, objects, and directories that may directly impact system functionality and/or performance, or that contain sensitive information. 3. Data stored in the information system must be protected with system access controls and must be encrypted when residing in non-secure areas.		**AC-03: Access Enforcement** Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	
Control	**N/A**	**Control**	**Individual Access**
New NIST SP 800-53 Rev.5 control and applicable to ARC-AMPE.		**AC-03(14): Individual Access** Provide organization-defined mechanisms to enable individuals to have access to the following elements of their Personally Identifiable Information (PII): PII / Protected Health Information (PHI) elements defined in applicable security/privacy plans.	

EDE		ARC-AMPE	
Control	**Information Flow Enforcement**	**Control**	**Information Flow Enforcement**
AC-4: Information Flow Enforcement The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy. **Implementation Standard** Organizations commonly employ information flow control policies and enforcement mechanisms to control the flow of information between designated sources and destinations (e.g., networks, individuals, and devices) within information systems and between interconnected systems. Flow control is based on the characteristics of the information and/or the information path. Enforcement occurs, for example, in boundary protection devices (e.g., gateways, routers, guards, encrypted tunnels, firewalls) that employ rule sets or establish configuration settings that restrict information system services, provide a packet-filtering capability based on header information, or message-filtering capability based on message content (e.g., implementing key word searches or using document characteristics). Organizations also consider the trustworthiness of filtering/inspection mechanisms (i.e., hardware, firmware, and software components) that are critical to information flow enforcement. NIST SP 800-53 control enhancements 3 through 22, while not present in this SSPP workbook, provide guidance on cross-domain solution needs which focus on more advanced filtering techniques, in-depth analysis, and stronger flow enforcement mechanisms implemented in cross-domain products, for example, high-assurance guards. Such capabilities are generally not available in commercial-off-the-shelf (COTS) information technology products.		**AC-04: Information Flow Enhancement** Enforce approved authorizations for controlling the flow of information within the system and between connected systems based on organization-defined information flow control policies.	

EDE		ARC-AMPE	
Control	**Separation of Duties**	**Control**	**Separation of Duties**
AC-5: Separation of Duties The organization: a. Separates duties of individuals as necessary (defined in the applicable security plan), to prevent malevolent activity; b. Documents separation of duties; and c. Defines information system access authorizations to support separation of duties. d. Enforces role-based access control policies over all subjects and objects where the policy specifies that: 1. The policy is uniformly enforced across all subjects and objects within the boundary of the IS; and 2. A subject that has been granted access to information is constrained from doing any of the following: a. Passing the information to unauthorized subjects or objects; b. Granting its privileges to other subjects; c. Changing one or more security attributes on subjects, objects, the information system, or information system components; d. Choosing the security attribute and attribute values to be associated with newly created or modified objects. e. Changing the rules governing access control. **Implementation Standards** 1. Audit functions must not be performed by security personnel responsible for administering access control. 2. Maintain a limited group of administrators with access based upon the users' roles and responsibilities. 3. The critical mission functions and information system support functions must be divided among separate individuals. 4. The information system testing functions (i.e., user acceptance, quality assurance, information security) and production functions must be divided among separate individuals or groups. 5. An independent entity, not the Business Owner, ISSO, System Developer(s)/Maintainer(s), or System administrator(s) responsible for the information system, conducts information security testing of the information system. 6. Assign user accounts and authenticators in accordance with role-based access control policies. 7. Configure the system to request user ID and authenticator prior to system access 8. Configure databases containing federal information in accordance with the organizational security administration guide to provide role-based access controls enforcing assigned privileges and permissions at the file, table, row, column, or cell level, as appropriate.		**AC-05: Separation of Duties** a. Identify and document organization-defined duties of individuals requiring separation; and b. Define system access authorizations to support separation of duties.	
Control	**Least Privilege**	**Control**	**Least Privilege**

EDE	ARC-AMPE
AC-6: Least Privilege The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned tasks in accordance with the organization's missions and business functions. This control supports and aligns with the provisions of the ACA and the requirements of 45 CFR §155.260, Privacy and security of personally identifiable information. **Implementation Standards** 1. Disable all file system access not explicitly required for system, application, and administrator functionality. 2. Contractors must be provided with minimal system and physical access and must agree to and support the organizational security requirements. The contractor selection process must assess the contractor's ability to adhere to and support the organization's security policy. 3. Restrict the use of database management utilities to only authorized database administrators. Prevent users from accessing database data files at the logical data view, field, or field-value level. Implement table-level access control. 4. Ensure that only authorized users are permitted to access those files, directories, drives, workstations, servers, network shares, ports, protocols, and services that are expressly required for the performance of job duties. 5. Disable all system and removable media boot access unless it is explicitly authorized by the CIO for compelling operational needs. If system and removable media boot access is authorized, boot access is password protected.	**AC-06: Least Privilege** Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.
Control **Authorize Access to Security Functions**	**Control** **Authorize Access to Security Functions**
AC-6(1): Authorize Access to Security Functions At a minimum, the organization explicitly authorizes access to organization-defined list of security functions (deployed in hardware, software, and firmware) to include the following list of security functions and security-relevant information for all system components: a. Setting/modifying audit logs and auditing behavior; b. Setting/modifying boundary protection system rules; c. Configuring/modifying access authorizations (i.e., permissions, privileges); d. Setting/modifying authentication parameters; and Setting/modifying system configurations and parameters.	**AC-06(01): Authorize Access to Security Functions** Authorize access for organization-defined individuals or roles to: a. Organization-defined security functions (deployed in hardware, software, and firmware); and b. Organization-defined security-relevant information, including but not limited to: 1. Setting/modifying audit logs and auditing behavior; 2. Setting/modifying boundary protection system rules; 3. Configuring/modifying access authorizations (i.e., permissions, privileges); 4. Setting/modifying authentication parameters; and 5. Setting/modifying system configurations and parameters.
Control **Non-Privileged Access for Non-Security Functions**	**Control** **Non-privileged Access for Nonsecurity Functions**
AC-6(2): Non-Privileged Access for Non-Security Functions At a minimum, the organization requires that users of information system accounts, or roles, with access to all security functions use non-privileged accounts, or roles, when	**AC-06(02): Non-privileged Access for Nonsecurity Functions** Require that users of system accounts (or roles) with access to organization-defined security functions or security-relevant

EDE		ARC-AMPE	
accessing other system functions, and if feasible, audits any use of privileged accounts, or roles, for such functions. This includes the following list of security functions or security-relevant information: a. Setting/modifying audit logs and auditing behavior; b. Setting/modifying boundary protection system rules; c. Configuring/modifying access authorizations (i.e., permissions, privileges); d. Setting/modifying authentication parameters; and e. Setting/modifying system configurations and parameters.		information use non-privileged accounts (or roles) when accessing nonsecurity functions.	
Control	**Privileged Accounts**	**Control**	**Privileged Accounts**
AC-6(5): Privileged Accounts The organization restricts privileged accounts on the information system to defined personnel or roles (defined in the applicable security plan).		**AC-06(05): Privileged Accounts** The organization restricts privileged accounts on the information system to defined organization-personnel or roles.	
Control	**N/A**	**Control**	**Review of User Privileges**
Existing NIST SP 800-53 Rev.4 control and new to ARC-AMPE.		**AC-06(07): Review of User Privileges** a. Review no less often than every ninety (90) days the privileges assigned to all users with privileges to validate the need for such privileges; and b. Reassign or remove privileges, if necessary, to correctly reflect organizational mission and business needs.	
Control	**Auditing Use of Privileged Functions**	**Control**	**Log Use of Privileged Functions**
AC-6(9): Auditing Use of Privileged Functions The information system audits the execution of privileged functions.		**AC-06(09): Log Use of Privileged Functions** Log the execution of privileged functions.	
Control	**Prohibit Non-Privileged Users from Executing Privileged Functions**	**Control**	**Prohibit Non-privileged Users from Executing Privileged Functions**
AC-6(10): Prohibit Non-Privileged Users from Executing Privileged Functions The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.		**AC-06(10): Prohibit Non-privileged Users from Executing Privileged Functions** Prevent non-privileged users from executing privileged functions.	
Control	**Unsuccessful Logon Attempts**	**Control**	**Unsuccessful Logon Attempts**
AC-7: Unsuccessful Logon Attempts The information system: a. Enforces the limit of consecutive invalid login attempts by a user specified in the Implementation Standard during the time period specified in the Implementation Standard; and b. Automatically disables or locks the account/node until released by an administrator or after the time period		**AC-07: Unsuccessful Logon Attempts** a. Enforce a limit of five (5) consecutive invalid logon attempts by a user during a fifteen (15) minute time period; and b. Automatically lock the account or node for a minimum of thirty (30) minutes or lock the account or node until released by an administrator or delay next logon prompt consistent with a delay algorithm or notify system administrator or take other action as determined by the	

EDE		ARC-AMPE	
specified in the Implementation Standard when the maximum number of unsuccessful attempts is exceeded. **Implementation Standards** 1. Enforces a limit of not more than three (3) consecutive invalid login attempts by a user during a fifteen (15) minute time; and 2. Automatically locks the account/node for thirty (30) minutes when the maximum number of unsuccessful attempts is exceeded. The control applies regardless of whether the login occurs via a local or network connection.		organization when the maximum number of unsuccessful attempts is exceeded.	
Control	**System Use Notification**	**Control**	**System Use Notification**
AC-8: System Use Notification The information system: a. Displays an approved system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. The approved banner states: *"This warning banner applies to the entirety of this system, meaning (1) this computer network, (2) all computers connected to this network, including this one, and (3) all devices and storage media attached to this network or to a computer on this network. This system is provided for authorized [Organization name] use only. Unauthorized or improper use of this system is prohibited and may result in disciplinary action and/or civil and criminal penalties.* *By using this system, you understand and consent to the following:* *[Organization name] may monitor, record, and audit your system usage. Therefore, you have no reasonable expectation of privacy regarding any communication or data transiting or stored on this system.* *At any time, and for any lawful purpose, [Organization name] may monitor, intercept, and search and seize any communication or data transiting or stored on this system. Any communication or data transiting or stored on this system may be disclosed or used for any lawful [Organization name] purpose."* b. Retains the notification message or banner on the screen until users take explicit actions to log on to or further access the information system; and c. For publicly accessible systems: 1. Displays system use information when appropriate, before granting further access; 2. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and 3. Includes a description of the authorized uses of the system.		**AC-08: System Use Notification** a. Display organization-defined system use notification message or banner to users before granting access to the system that provides privacy and security notices consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines and state that: 1. Users are accessing a system that contains U.S. Government information; 2. System usage may be monitored, recorded, and subject to audit; 3. Unauthorized use of the system is prohibited and subject to criminal and civil penalties; and 4. Use of the system indicates consent to monitoring and recording; b. Retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the system; and c. For publicly accessible systems: 1. Display system use information organization-defined conditions before granting further access to the publicly accessible system; 2. Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and 3. Include a description of the authorized uses of the system.	

EDE		ARC-AMPE	
Implementation Standards 1. The System Owner determines elements of the environment that require the System Use Notification control. 2. The System Owner determines how System Use Notification will be verified and provides appropriate periodicity of the check. 3. If not performed as part of a Configuration Baseline check, the organization has a documented agreement on how to provide results of verification and the necessary periodicity of the verification by the service provider.			
Control	**Concurrent Session Control**	**Control**	**Concurrent Session Control**
AC-10: Concurrent Session Control The information system limits the number of concurrent sessions for each system account to one (1) session for both normal and privileged users.		**AC-10: Concurrent Session Control** Limit the number of concurrent sessions for each account and/or account types to one (1) session.	
Control	**Session Lock**	**Control**	**Device Lock**
AC-11: Session Lock The information system: a. Prevents further access to the system by initiating a session lock after fifteen (15) minutes of inactivity (for both remote and internal access connections) or upon receiving a request from a user; and b. Retains the session lock until the user reestablishes access using established identification and authentication procedures. **Implementation Standard** Period of inactivity must be no more than 15 minutes before session lock occurs for remote and mobile devices and requires re-authentication. As organizations continue to migrate to laptops and docking stations making clients increasingly mobile, this is a logical extension of that requirement.		**AC-11: Device Lock** a. Prevent further access to the system by initiating a device lock after fifteen (15) minutes of inactivity; requiring the user to initiate a device lock before leaving the system unattended; and b. Retain the device lock until the user reestablishes access using established identification and authentication procedures.	
Control	**Pattern-Hiding Displays**	**Control**	**N/A**
AC-11(1): Pattern-Hiding Displays The information system conceals, via the session lock, information previously visible on the display with a publicly viewable image.		**Withdrawn Control**: No longer required for the minimum baseline but should still be considered a best practice.	
Control	**Session Termination**	**Control**	**Session Termination**
AC-12: Session Termination The information system automatically terminates a user session after defined conditions or trigger events (defined in the system security plan) requiring session disconnect.		**AC-12: Session Termination** Automatically terminate a user session after organization-defined conditions or trigger events requiring session disconnect.	

EDE		ARC-AMPE	
Control	**N/A**	**Control**	**User-Initiated Logouts**
Existing NIST SP 800-53 Rev.4 control which was not selected for EDE and is applicable to ARC-AMPE.		**AC-12(01): User-Initiated Logouts** Provide a logout capability for user-initiated communications sessions whenever authentication is used to gain access to organization-defined information resources.	
Control	**N/A**	**Control**	**Termination Message**
New NIST SP 800-53 Rev.5 control and applicable to ARC-AMPE.		**AC-12(02): Termination Message** Display an explicit logout message to users indicating the termination of authenticated communications sessions.	
Control	**N/A**	**Control**	**Timeout Warning Message**
New NIST SP 800-53 Rev.5 control and applicable to ARC-AMPE.		**AC-12(03): Timeout Warning Message** Display an explicit message to users indicating that the session will end in an organization-defined time until end of session.	
Control	**Permitted Actions without Identification or Authentication**	**Control**	**Permitted Action Without Identification or Authentication**
AC-14: Permitted Actions without Identification or Authentication The organization: a. Identifies specific user actions that can be performed on the information system without identification or authentication; b. Documents and provides supporting rationale in the system security plan for user actions not requiring identification or authentication; and Configures Information systems to permit public access without first requiring individual identification and authentication only to the extent necessary to accomplish mission objectives.		**AC-14: Permitted Actions Without Identification or Authentication** a. Identify organization-defined user actions that can be performed on the system without identification or authentication consistent with organizational mission and business functions; and Document and provide supporting rationale in the security plan for the system, user actions not requiring identification or authentication.	
Control	**Remote Access**	**Control**	**Remote Access**
AC-17: Remote Access The organization monitors for unauthorized remote access to the information system (including access to internal networks by VPN). Remote access for privileged functions must be permitted only for compelling operational needs, must be strictly controlled, and must be explicitly authorized, in writing, by the organization CIO or his/her designated representative. If remote access is authorized, the organization: a. Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; b. Authorizes remote access to the information system prior to allowing such connections; and c. Monitors for unauthorized remote access to the information system: 1. Personally-owned equipment must be scanned before being connected to the organization		**AC-17: Remote Access** a. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and b. Authorize each type of remote access to the system prior to allowing such connections.	

<table>
<tr><th colspan="2">EDE</th><th colspan="2">ARC-AMPE</th></tr>
<tr><td colspan="2">systems or networks to ensure compliance with the organization requirements; and
2. Personally-owned equipment must be prohibited from processing, accessing, or storing organization sensitive information unless it is approved in writing by the organization Senior Official for Privacy (SOP) and employs required encryption (FIPS 140-2 validated module).

Implementation Standards
1. Require callback capability with re-authentication to verify connections from authorized locations when the Medicare Data Communications Network (MDCN) or Multi-Protocol Label Switching (MPLS) service network cannot be used. For application systems and turnkey systems that require the vendor to log-on, the vendor will be assigned a User ID and password and enter the network through the standard authentication process. Access to such systems will be authorized and logged. User IDs assigned to vendors will be recertified within every three hundred sixty-five (365) days.
2. If e-authentication is implemented as a remote access solution or associated with remote access, refer to the most recent NIST SP 800-63.
3. All computers and devices, whether organization-furnished equipment or contractor-furnished equipment, that require any network access to a network or system are securely configured and meet at a minimum, the following security requirements:
a. Up-to-date system patches;
b. Current anti-virus software;
c. Host-based intrusion detection system;
d. Functionality that provides the capability for automatic execution of code disabled; and
e. Employs required encryption (FIPS 140-2 validated module).
4. For organizations supporting remote access (including teleworking), ensure NIST SP 800-46 guidelines are followed by defining policies and procedures that define:
a. Forms of permitted remote access;
b. Types of devices permissible for remote access;
c. Type of access remote users are granted; and
d. How remote user account provisioning is handled.
5. Remote connection for privileged functions must be performed using multi-factor authentication.</td><td colspan="2"></td></tr>
<tr><td>Control</td><td>Automated Monitoring/Control</td><td>Control</td><td>Monitoring and Control</td></tr>
<tr><td colspan="2">AC-17(1): Automated Monitoring/Control
The information system monitors and controls remote access methods.

Implementation Standards
The organization implements organization and industry best practice distributed blocking rules within one hour of receipt.</td><td colspan="2">AC-17(01): Monitoring and Control
Employ automated mechanisms to monitor and control remote access methods.</td></tr>
</table>

EDE		ARC-AMPE	
Control	**Protection of Confidentiality/Integrity Using Encryption**	**Control**	**Protection of Confidentiality and Integrity Using Encryption**
AC-17(2): Protection of Confidentiality/Integrity Using Encryption The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.		**AC-17(02): Protection of Confidentiality and Integrity Using Encryption** Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.	
Control	**Managed Access Control Points**	**Control**	**Managed Access Control Points**
AC-17(3): Managed Access Control Points The information system routes all remote accesses through a limited number of managed access control points.		**AC-17(03): Managed Access Control Points** Route remote accesses through authorized and managed network access control points.	
Control	**Privileged Commands/Access**	**Control**	**Privileged Commands and Access**
AC-17(4): Privileged Commands/Access The organization: a. Authorizes the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs; and b. Documents the rationale for such access in the security plan for the information system.		**AC-17(04): Privileged Commands and Access** a. Authorize the execution of privileged commands and access to security-relevant information via remote access only in a format that provides assessable evidence and for compelling operational needs; and b. Document the rationale for remote access in the security plan for the system.	
Control	**Disconnect/Disable Access**	**Control**	**Disconnect or Disable Access**
AC-17(9): Disconnect/Disable Access The organization provides the capability to expeditiously disconnect or disable remote access to the information system within 15 minutes. **Implementation Standards** The organization terminates or suspends network connections (i.e., a system-to-system interconnection) upon issuance of an order by the CIO, CISO, or Senior Official for Privacy (SOP).		**AC-17(09): Disconnect or Disable Access** Provide the capability to disconnect or disable remote access to the system within one (1) hour.	
Control	**Wireless Access**	**Control**	**Wireless Access**
AC-18: Wireless Access The organization monitors for unauthorized wireless access to information systems and prohibits the installation of wireless access points (WAP) to information systems unless explicitly authorized, in writing, by the organization CIO or a designated representative. If wireless access is authorized, the organization: a. Establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access; b. Authorizes wireless access to the information system prior to allowing such connections; c. The organization ensures that:		**AC-18: Wireless Access** a. Establish configuration requirements, connection requirements, and implementation guidance for each type of wireless access; and b. Authorize each type of wireless access to the system prior to allowing such connections.	

<table>
<tr><th colspan="2">EDE</th><th colspan="2">ARC-AMPE</th></tr>
<tr><td colspan="2">1. The organization CIO must approve and distribute the overall wireless plan for his or her respective organization; and
2. Mobile and wireless devices, systems, and networks are not connected to wired organization networks except through appropriate controls (e.g., VPN port) or unless specific authorization from the organization network management has been received.
Implementation Standards
1. If wireless access is explicitly authorized, wireless device service set identifier broadcasting is disabled and the following wireless restrictions and access controls are implemented:
a. Encryption protection is enabled;
b. Access points are placed in secure areas;
c. Access points are shut down when not in use (i.e., nights, weekends);
d. A firewall is implemented between the wireless network and the wired infrastructure;
e. MAC address authentication is utilized;
f. Static IP addresses, not Dynamic Host Configuration Protocol (DHCP), is utilized;
g. Personal firewalls are utilized on all wireless clients;
h. File sharing is disabled on all wireless clients;
i. Intrusion detection agents are deployed on the wireless side of the firewall;
j. Wireless activity is monitored and recorded, and the records are reviewed on a regular basis;
k. Organizational policy related to wireless client access configuration and use is documented;
2. Wireless printers and all Bluetooth devices such as keyboards are not allowed without explicit approval by the organization’s Authorizing Official (AO).</td><td colspan="2"></td></tr>
<tr><td>Control</td><td>Authentication and Encryption</td><td>Control</td><td>Authentication and Encryption</td></tr>
<tr><td colspan="2">AC-18(1): Authentication and Encryption
If wireless access is explicitly authorized, the information system protects wireless access to the system using encryption and authentication of both users and devices.</td><td colspan="2">AC-18(01): Authentication and Encryption
Protect wireless access to the system using authentication of users, devices, and encryption.</td></tr>
<tr><td>Control</td><td>N/A</td><td>Control</td><td>Disable Wireless Networking</td></tr>
<tr><td colspan="2">Existing NIST SP 800-53 Rev.4 control which was not selected for EDE and is applicable to ARC-AMPE.</td><td colspan="2">AC-18(03): Disable Wireless Networking
Disable, when not intended for use, wireless networking capabilities embedded within system components prior to issuance and deployment.</td></tr>
<tr><td>Control</td><td>Access Control for Mobile Devices</td><td>Control</td><td>Access Control for Mobile Devices</td></tr>
</table>

EDE		ARC-AMPE	
AC-19: Access Control for Mobile Devices The organization: a. Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices; b. Authorizes, through the organization CIO, the connection of mobile devices to organizational information systems **Implementation Standard** Encrypt information on all mobile devices that contains PII.		**AC-19: Access Control for Mobile Devices** a. Establish configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices, to include when such devices are outside of controlled areas; and b. Authorize the connection of mobile devices to organizational systems.	
Control	**Full-Device / Container-Based Encryption**	**Control**	**Full Device and Container-based Encryption**
AC-19(5): Full-Device / Container-Based Encryption The organization employs the required (FIPS 140-2 validated module) full-device encryption or container encryption to protect the confidentiality and integrity of information on approved mobile devices. **Implementation Standards** Encrypt information on all mobile devices that contain PII.		**AC-19(05): Full Device and Container-based Encryption** Employ full device encryption or container encryption using the most current FIPS 140-compliant encryption standards to protect the confidentiality and integrity of information on approved mobile devices.	
Control	**Use of External Information Systems**	**Control**	**Use of External Systems**
AC-20: Use of External Information Systems The organization prohibits the use of external information systems, including but not limited to, Internet kiosks, personal desktop computers, laptops, tablet personal computers, personal digital assistant (PDA) devices, cellular telephones, facsimile machines, and equipment available in hotels or airports to store, access, transmit, or process sensitive information, unless explicitly authorized, in writing, by the organization CIO or his/her designated representative. If external information systems are authorized, the organization establishes strict terms and conditions for their use. The terms and conditions must address, at a minimum: a. The types of applications that can be accessed from external information systems; b. The maximum FIPS 199 security category of information that can be processed, stored, and transmitted; c. How other users of the external information system will be prevented from accessing federal information; d. The use of VPN and stateful inspection firewall technologies; e. The use of and protection against the vulnerabilities of wireless technologies; f. The maintenance of adequate physical security controls; g. The use of virus and spyware protection software; and h. How often the security capabilities of installed software are to be updated. **Implementation Standards** 1. Instruct all personnel working from home to implement fundamental security controls and practices, including		**AC-20: Use of External Systems** a. Establish organization-defined terms and conditions and identify organization-defined controls asserted to be implemented on external systems, consistent with the trust relationships established with other organizations owning, operating, and/or maintaining external systems, allowing authorized individuals to: 1. Access the system from external systems; and 2. Process, store, or transmit organization-controlled information using external systems; or Prohibit the use of organizationally defined types of external systems.	

EDE		ARC-AMPE	
passwords, virus protection, and personal firewalls. Limit remote access only to information resources required by home users to complete job duties. Require that any organization-owned equipment be used only for business purposes by authorized employees. 2. Only organization owned computers and software can be used to process, access, and store PII. 3. Privacy requirements must be addressed in agreements that cover relationships in which external information systems are used to access, process, store, or transmit and manage PII. Access to PII from external information systems (including, but not limited to, personally owned information systems/devices) is limited to those organizations and individuals with a binding agreement to terms and conditions of privacy requirements which protect the PII.			
Control	**Limits on Authorized Use**	**Control**	**Limits on Authorized Use**
AC-20(1): Limits on Authorized Use The organization permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization: a. Verifies the implementation of required security controls on the external system as specified in the organization's information security policy and security plan; or b. Retains approved information system connection or processing agreements with the organizational entity hosting the external information system.		**AC-20(01): Limits on Authorized Use** Permit authorized individuals to use an external system to access the system or to process, store, or transmit organization-controlled information only after: a. Verification of the implementation of controls on the external system as specified in the organization's security and privacy policies and security and privacy plans; or b. Retention of approved system connection or processing agreements with the organizational entity hosting the external system.	
Control	**Portable Storage Devices**	**Control**	**Portable Storage Devices — Restricted Use**
AC-20(2): Portable Storage Devices The organization restricts the use of organization-controlled portable storage devices by authorized individuals on external information systems.		**AC-20(02): Portable Storage Devices — Restricted Use** Restrict the use of organization-controlled portable storage devices by authorized individuals on external systems using organization-defined restrictions.	
Control	**Information Sharing**	**Control**	**Information Sharing**
AC-21: Information Sharing The organization: a. Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for approved information-sharing circumstances where user discretion is required; and b. Employs defined automated mechanisms or manual processes (defined in the applicable security plan) to assist users in making information-sharing/collaboration decisions.		**AC-21: Information Sharing** a. Enable authorized users to determine whether access authorizations assigned to a sharing partner match the information's access and use restrictions for organization-defined information-sharing circumstances where user discretion is required; and b. Employ organization-defined automated mechanisms or manual processes to assist users in making information-sharing and collaboration decisions.	

EDE		ARC-AMPE	
Control	**Publicly Accessible Content**	**Control**	**Publicly Accessible Content**
AC-22: Publicly Accessible Content The organization: a. Designates individuals authorized to post information onto a publicly accessible information system; b. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information; c. Reviews the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included; and d. Reviews the content on the publicly accessible information system for nonpublic information at least quarterly and removes such information, if discovered. **Implementation Standard** The organization reviews the content on the publicly accessible organizational information system for nonpublic information at least quarterly		**AC-22: Publicly Accessible Content** a. Designate individuals authorized to make information publicly accessible; b. Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information; c. Review the proposed content of information prior to posting onto the publicly accessible system to ensure that nonpublic information is not included; and d. Review the content on the publicly accessible system for nonpublic information bi-weekly (no less often than fourteen [14] days) and remove such information, if discovered.	

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 (Access Control (AC))_07142025