Centers for Medicare & Medicaid Services
Center for Consumer Information and
Insurance Oversight

Acceptable Risk Controls for Affordable Care Act (ACA), Medicaid, and Partner Entities (ARC-AMPE)

ARC-AMPE: Volume I

Final

Version 1.02

April 10, 2025

Record of Changes

Version	Date	Author / Owner	Description of Change
1.0	March 04, 2025	CMS	Version 1.0 for public release
1.01	March 10, 2025	CMS	Updated text to refer to recently posted versions of guidance that informed ARC-AMPE. No changes to the controls
1.02	April 10, 2025	CMS	Updated for 508 compliance

Foreword

The Patient Protection and Affordable Care Act (hereafter the "Affordable Care Act" or "ACA"), requires that each state develop its own Health Insurance Exchange or default to the Federally-facilitated Exchange (FFE, also known as the "Marketplace").[1] Exchanges[2] provide organized marketplaces where consumers and small businesses can compare available health plan options based on price, benefits, and services. The Department of Health and Human Services (HHS) and the Centers for Medicare & Medicaid Services (CMS) within HHS are responsible for implementing many provisions of the ACA, including setting security and privacy standards[3] and overseeing and monitoring the Exchanges and certain non-Exchange entities for compliance with these privacy and security standards.[4]

CMS has developed a set of standards for managing security and privacy risks of the Exchanges, including the *Minimum Acceptable Risk Standards for Exchanges (MARS-E)* and *Non-Exchange Entity Governance, Risk Management, and Compliance (NEE GRC)*.[5] The *Acceptable Risk Controls for ACA, Medicaid, and Partner Entities (ARC-AMPE)* is the next iteration of security and privacy standards to address the complex business and regulatory environment of the Exchanges.[6] ARC-AMPE incorporates updates to federal laws, agency regulations, and the latest National Institute of Standards and Technology (NIST) standards and guidelines. ARC-AMPE includes technical controls that may facilitate adherence to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) requirements.[7] ARC-AMPE accommodates the evolving ACA environment, including new entities, functions, and technology advancements governing both business functions and security safeguards. ARC-AMPE integrates enterprise risk management (ERM) to provide a comprehensive approach to manage risks.

All ARC-AMPE users[8] must review *ARC-AMPE Volume I*. ARC-AMPE users who are an ACA Administering Entity (ACA AE)[9] or a select Partner Entity[10] are required to comply with *ARC-AMPE Volume II*[11] and complete accompanying artifacts to document their compliance with

[1] Sections 1311(b) and 1321(c) of the ACA. See also 45 CFR §§155.100(a), 155.105(f).

[2] For the purposes of this document, "Exchanges" includes FFEs, State-based Exchanges (SBEs), and SBEs on the federal platform (SBE-FPs). Subsection 1.3.1 provides further information regarding Exchanges.

[3] 45 CFR. §§155.260 sets forth the privacy and security safeguards of Personally Identifiable Information (PII).

[4] See 45 CFR §155.280.

[5] The *Minimum Acceptable Risk Standards for Exchanges (MARS-E)* were applicable to ACA Administering Entities while the *Non-Exchange Entity Governance, Risk Management, and Compliance (NEE GRC) Framework* was applicable to Non-Exchange Entities. ACA Administering Entities and Non-Exchange Entities are defined in Subsection 1.3.2.

[6] *ARC-AMPE* supersedes and replaces *MARS-E* and the *NEE GRC Framework* effective upon publication.

[7] Requirements include the HIPAA Security, Privacy, and Breach Notification rules. This document does not provide HIPAA guidance; entities should work with their own counsel to determine the applicability of HIPAA to their organization.

[8] Subsection 1.3.2 includes a definition of ARC-AMPE users.

[9] Subsection 1.3.2 includes a definition of ACA Administering Entity.

[10] Subsection 1.3.2 includes a definition of Partner Entities.

[11] *ARC-AMPE Volume II* is the System Security and Privacy Plan (SSPP) template with required baseline controls.

ARC-AMPE Volume II.[12] All other ARC-AMPE users may leverage *ARC-AMPE Volume II*[13] as an informative reference to bolster their security and privacy posture, facilitate adherence to applicable HIPAA requirements, and safeguard consumer[14] or beneficiary[15] PII.[16]

ARC-AMPE Volumes I and *II* will be reviewed and updated as required to ensure the protection of consumer or beneficiary PII against risks and threats. All changes to *ARC-AMPE Volume I* and *II* must be approved by the CMS Chief Information Officer and the CMS Chief Information Security Officer (CMS Senior Agency Official for Privacy).

ARC-AMPE Volumes I and *II* have been reviewed in accordance with *CMS Information Systems Security and Privacy Policy (IS2P2)*[17] policy and have been approved for publication.

/s/
Keith Busby Date
Acting Chief Information Security Officer
Centers for Medicare & Medicaid Services

/s/
George Hoffmann Date
Acting Chief Information Officer
Centers for Medicare & Medicaid Services

[12] Refer to Section 3 for information on which ARC-AMPE users are subject to mandatory compliance with *ARC-AMPE Volume II.*

[13] Legal agreements with ARC-AMPE users may stipulate that an ARC-AMPE user that is not required to comply with *ARC-AMPE Volume II* under statute or regulations must comply by virtue of contract.

[14] The ACA does not explicitly define the term "consumer" in a specific, standalone definition section. However, throughout the ACA, the term "consumer" is generally used to refer to individuals who are purchasing or using health insurance and healthcare services.

[15] Beneficiary means a person who is entitled to Medicare benefits and/or has been determined to be eligible for Medicaid. 42 CFR § 400.200 General definitions.

[16] PII includes Protected Health Information (PHI). These terms are further explained in Subsection 1.3.3.

[17] See https://security.cms.gov/policy-guidance/cms-information-systems-security-privacy-policy-is2p2.

Table of Contents

List of Figures

List of Tables

1. Introduction

The Patient Protection and Affordable Care Act (hereafter the "Affordable Care Act" or "ACA"), requires that each state develop its own Health Insurance Exchange or default to the Federally-facilitated Exchange (FFE, also known as the "Marketplace").[18] Exchanges[19] provide organized marketplaces where consumers[20] and small businesses can compare available plan options based on price, benefits, and services. Strong security and privacy protections are necessary to meet applicable statutory and regulatory requirements;[21] protect and ensure the confidentiality, integrity, and availability of Exchange information, including enrollment information, and associated information systems; and establish public trust and confidence that individuals' Personally Identifiable Information (PII)[22] will be protected.

The Department of Health and Human Services (HHS) and the Centers for Medicare & Medicaid Services (CMS) within HHS are responsible for implementing many provisions of the ACA, including facilitating eligibility determinations, exemptions, and enrollment in health insurance coverage and insurance affordability programs.[23] HHS and CMS are also responsible for providing security and privacy standards[24] and overseeing and monitoring Exchanges and certain Non-Exchange Entities (NEEs) for compliance with these privacy and security standards.[25]

CMS provides business, information, and technical guidance, and creates common baselines and standards for information system implementation activities. CMS originally developed a set of standards for ACA Administering Entities (ACA AEs) and NEEs to manage security and privacy risks of the Exchanges.[26] CMS expanded these standards to accommodate evolving ACA functions[27], the increasing number of entities supporting ACA functions, and technology advancements governing both business functions and security safeguards. The resulting enhanced security and privacy standards documented in the *Acceptable Risk Controls for ACA, Medicaid, and Partner Entities (ARC-AMPE)* respond to the complex and dynamic business and regulatory environment of the Exchanges. ARC-AMPE incorporates updates to federal laws, agency regulations, and the latest National Institute of Standards and Technology (NIST) standards and guidelines. ARC-AMPE also includes technical requirements that may apply to

[18] Sections 1311(b) and 1321(c) of the ACA. See also 45 CFR §§155.100(a), 155.105(f).

[19] Subsection 1.3.1 provides further information regarding Exchanges.

[20] The ACA does not explicitly define the term "consumer" in a specific, standalone definition section. However, throughout the ACA, the term "consumer" is generally used to refer to individuals who are purchasing or using health insurance and healthcare services.

[21] See, e.g., sections 1411(g), 1413(c)(2), and 1414(a)(1) of the ACA; 45 CFR §155.260.

[22] Office of Management and Budget (OMB) Memorandum M-17-12 (January 3, 2017) defines "Personally Identifiable Information (PII)" as "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual." Individually Identifiable Health Information (IIHI) and Protected Health Information (PHI) are included in the definition of PII. Subsection 1.3.3 provides additional explanation of this concept.

[23] See generally 45 CFR Part 155.

[24] See 45 CFR §155.260.

[25] See 45 CFR §155.280.

[26] The *Minimum Acceptable Risk Standards for Exchanges (MARS-E)* governed ACA Administering Entities while the *Non-Exchange Entity Governance, Risk Management, and Compliance (NEE GRC) Framework* governed Non-Exchange Entities. ACA Administering Entities and Non-Exchange Entities are defined in Subsection 1.3.2.

[27] ACA functions include but are not limited to methods to protect consumer or beneficiary PII, expand access to health insurance coverage through the Exchanges, and reduce healthcare costs for Exchange consumers.

ARC-AMPE users that are Health Insurance Portability and Accountability Act of 1996 (HIPAA) Business Associates (BAs) or Covered Entities (CEs).[28] ARC-AMPE integrates enterprise risk management (ERM) to provide a comprehensive approach to manage risks.

1.1 Purpose and Scope

ARC-AMPE is the CMS framework by which ARC-AMPE users may or must (as applicable) manage the security and privacy of the information systems they deploy to administer end-to-end operations throughout the health coverage eligibility and enrollment lifecycle. *ARC-AMPE Volume I* provides high-level guidance for adhering to the framework. *ARC-AMPE Volume II* establishes the minimum-level security and privacy controls for ARC-AMPE users to implement the framework to protect information within information systems. Information systems include all systems that have or are applying to have an authorized connection to the CMS Federal Data Services Hub (hereafter "the Hub") and/or access to PII contained within or PII derived from[29] the Exchange repositories.

All ARC-AMPE users[30] must review *ARC-AMPE Volume I*. ARC-AMPE users who are an ACA Administering Entity (ACA AE)[31] or a select Partner Entity[32] are required to comply with *ARC-AMPE Volume II*[33] and complete accompanying artifacts to document their compliance with *ARC-AMPE Volume II*.[34] All other ARC-AMPE users may leverage *ARC-AMPE Volume II*[35] as an informative reference to bolster their security and privacy posture, facilitate adherence to applicable HIPAA requirements, and safeguard consumer or beneficiary[36] PII.[37]

1.2 Authority

All federal agencies and their contractors must comply with various federal security and privacy laws and regulations depending on the types of data processed and certain other factors. Key federal security and privacy laws that are essential to understanding the basic requirements levied on federal agencies, state partners, contractors, and supporting commercial companies, include but are not limited to:

[28] Technical requirements include the HIPAA Security, Privacy, and Breach Notification rules. This document does not provide HIPAA guidance; entities should work with their own counsel to determine the applicability of HIPAA to their organization.

[29] PII derived from Exchange repositories refers to PII that has been transmitted from an Exchange repository to another repository to support non-ACA functions, e.g., dispute resolution.

[30] Subsection 1.3.2 includes a definition of ARC-AMPE users.

[31] Subsection 1.3.2 includes a definition of ACA Administering Entity.

[32] Subsection 1.3.2 includes a definition of Partner Entities.

[33] *ARC-AMPE Volume II* is the System Security and Privacy Plan (SSPP) template with required baseline controls.

[34] Refer to Section 3 for information on which ARC-AMPE users are subject to mandatory compliance with *ARC-AMPE Volume II*.

[35] Legal agreements with ARC-AMPE users may stipulate that an ARC-AMPE user that is not required to comply with *ARC-AMPE Volume II* under statute or regulations must comply by virtue of contract.

[36] Beneficiary means a person who is entitled to Medicare benefits and/or has been determined to be eligible for Medicaid. 42 CFR § 400.200 General definitions.

[37] PII includes Protected Health Information (PHI). These terms are further explained in Section 1.3.3.

- Privacy Act of 1974
- e-Government Act of 2002
- The Federal Information Security Modernization Act (FISMA) of 2014, which amends the Federal Information Security Management Act (FISMA) of 2002 (enacted as part of the e-Government Act of 2002)
- The ACA and implementing HHS Regulations
- The Office of Management and Budget (OMB) revised Circular A-130, *Managing Information as a Strategic Resource,* July 28, 2016
- Safeguards for Protecting Federal Tax Returns and Return Information (26 U.S.C. §6103 and related provisions)
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- Health Information Technology for Economic and Clinical Health Act (HITECH) of 2009

The security and privacy controls and implementation standards documented in *ARC-AMPE Volume II* are established in accordance with Section 1411(g) of the ACA (42 U.S.C. §18081(g)), FISMA of 2014 (44 U.S.C. §3551), and 45 CFR §155.260 (and consistent with the standards in 45 CFR §§155.260(a)(1) through (a)(6)).

45 CFR §155.260 requires Exchanges and NEEs to safeguard PII. It permits the creation, collection, use and disclosure of PII only for the performance of the functions of Exchanges (per 45 CFR §155.200), unless consumer consent is provided. These requirements apply to agencies administering Medicaid, Children's Health Insurance Program (CHIP), or a Basic Health Program (BHP) with respect to PII shared between Exchanges and such entities pursuant to 45 CFR §155.260(e) (which requires agreements between Exchanges and agencies administering Medicaid, CHIP, or the BHP for the exchange of eligibility information to meet any applicable requirements under 45 CFR §155.260).

Section 155.260(a)(3) requires Exchanges to establish and implement security and privacy standards consistent with the Fair Information Practice Principles (FIPPs). The FIPPs are a collection of widely accepted principles that organizations use when evaluating information systems, processes, programs, and activities that affect individual privacy. The eight FIPPs are (1) Individual Access; (2) Correction; (3) Openness and Transparency; (4) Individual Choice; (5) Collection, Use and Disclosure Limitations; (6) Data Quality and Integrity; (7) Safeguards; and (8) Accountability.[38]

NEEs must comply with all security and privacy standards established by HHS pursuant to 45 CFR §155.260.[39] In addition, 45 CFR §155.260(b)(3)(i) provides that an Exchange must, among other things, require as a condition of contract or agreement with an NEE that the NEE comply with security and privacy standards that are consistent with the standards in 45 CFR §155.260, including being at least as protective as the standards the Exchange has established and implemented for itself.

[38] More information on FIPPs is available at: https://www.fpc.gov/resources/fipps/.

[39] See 45 CFR §155.260(b)(3).

Furthermore, 45 CFR §155.280(a) requires that HHS oversee and monitor the FFE, State-based Exchange-Federal Platforms (SBE-FPs), and NEEs for compliance with the security and privacy standards established and implemented by an FFE pursuant to 45 CFR §155.260. This provision also provides that SBEs will oversee and monitor NEEs that are required to comply with the security and privacy standards established and implemented by an SBE in accordance with 45 CFR §155.260.

HHS and CMS issue policies and standards that incorporate implementation guidance of the federal mandates. CMS based *ARC-AMPE Volume II* on *CMS Acceptable Risk Safeguards (ARS)*[40]; CMS Information Systems Security and Privacy Policy (IS2P2)[41], which incorporates guidance from HHS Information Security and Privacy Policy (IS2P)[42]; and Federal Risk and Authorization Management Program (FedRAMP)[43] guidance for cloud-based systems.

1.3 Key Concepts and Terms

1.3.1 Health Insurance Exchanges (Exchanges)

Exchanges allow consumers and small businesses in every state (including the District of Columbia) to obtain health and/or dental insurance coverage through the Individual or Small Business Health Options Program (SHOP) Health Insurance Exchanges operated by states through State-based Exchanges or operated by the federal government through the FFE. SBE-FPs are SBEs that rely on HHS to perform certain Exchange functions, specifically eligibility and enrollment, while still retaining responsibility for performing other Exchange functions such as Qualified Health Plan (QHP) certification and consumer outreach and assistance functions.[44]

For the purposes of this document, “Exchanges” includes FFEs, SBEs, and SBE-FPs.

1.3.2 ARC-AMPE Users

ARC-AMPE users include:

- **ACA Administering Entity** (ACA AE) – Exchanges, whether federal or state, state Medicaid agencies, state CHIP agencies, or state agencies administering a BHP.
- **Partner Entity** – An entity that is not an ACA AE that has authority to create, collect, use, or disclose Exchange consumer or beneficiary PII by either: (1) ACA regulation or (2) virtue of a legal or contractual agreement with CMS.
    - **Non-Exchange Entity** – Defined by ACA regulation as any individual or entity that: (1) gains access to PII submitted to an Exchange; or (2) collects, uses, or discloses PII gathered directly from applicants, qualified individuals, or enrollees, while that individual or entity is performing functions agreed to with the Exchange.[45] For the

[40] See https://security.cms.gov/policy-guidance/cms-acceptable-risk-safeguards-ars.

[41] See https://security.cms.gov/policy-guidance/cms-information-systems-security-privacy-policy-is2p2.

[42] In order to access the HHS IS2P, send an email to Fisma@hhs.gov or visit the HHS FISMA Working Group on the OMB Max Portal.

[43] Refer to https://www.fedramp.gov/assets/resources/documents/FedRAMP_Security_Controls_Baseline.xlsx.

[44] More information is available at: https://www.cms.gov/CCIIO/Resources/Fact-Sheets-and-FAQs/state-marketplaces.

[45] Non-Exchange Entity is defined in 45 CFR §155.260(b)(1).

purposes of ARC-AMPE, a NEE is a Partner Entity that supports ACA functions. NEEs may include but are not limited to:

- **Agent or Broker** – A person or entity licensed by the state as an agent, broker, or insurance producer.[46]
- **Web-Broker** – An individual agent or broker, group of agents or brokers, or business entity registered with an Exchange that develops and hosts a non-Exchange website that interfaces with an Exchange to assist consumers with direct enrollment in QHPs offered through the Exchange.[47]
- **Direct Enrollment (DE) Entity**[48] – An entity that supports the Classic Direct Enrollment (Classic DE) pathway and/or the Enhanced DE (EDE) pathway. A DE Entity assists consumers with direct enrollment in QHPs offered through the Exchange in a manner considered to be through the Exchange. An EDE Entity is a DE Entity approved by CMS to use the EDE pathway.[49]
  - **Primary EDE Entity** – An entity that develops, designs, and hosts its own EDE environment for its own use or for use by others.
  - **Upstream EDE Entity** – An entity that uses an EDE environment provided by a Primary EDE Entity. All Upstream EDE Entities must have a legal relationship with a Primary EDE Entity memorialized in a signed, written agreement between the Upstream EDE Entity and the Primary EDE Entity.

- **Service Provider** – A type of Partner Entity that accesses consumer or beneficiary PII to support CMS functions, which may or may not include ACA functions. Service providers may include, but are not limited to, entities that provide income verification, healthcare coverage verification, and dispute resolution.

- **State Healthcare Agency** – An entity that: (1) is not an ACA AE; (2) is not a Partner Entity; and (3) has access to consumer or beneficiary PII while performing health and human services functions that are not ACA functions. A State Healthcare Agency may be considered a HIPAA CE, a HIPAA BA, or a HIPAA Hybrid Entity.
- **Healthcare Organization** – Small, medium, and large healthcare entities[50] that support ACA AEs, Medicaid/CHIP, and State Healthcare Agencies. Healthcare organizations

[46] Agent or Broker is defined in 45 CFR §155.20.

[47] Web-broker is defined in 45 CFR §155.20.

[48] Direct Enrollment Entity is defined in 45 CFR §155.20.

[49] Classic Direct Enrollment, Classic Direct Enrollment Pathway, Direct Enrollment, Enhanced Direct Enrollment, Enhanced Direct Enrollment Entity, Enhanced Direct Enrollment Environment, Enhanced Direct Enrollment Pathway, Primary EDE Entity, and Upstream EDE Entity are defined in the EDE Business Agreement. See https://zone.cms.gov/document/enhanced-direct-enrollment-ede-documents-and-materials. Users must request access to zONE to view the EDE Business Agreement.

[50] Small, medium, and large healthcare organizations are characterized in Cybersecurity Act of 2015, Section 405(d). More information is available at: https://405d.hhs.gov/Documents/HICP-Main-508.pdf. Refer to Table 1, Selecting the “Best Fit” For Your Organization.

may be a HIPAA CE or a HIPAA BA.[51] CMS may determine that select healthcare organizations are Partner Entities.[52]

- **Small** – Generally, these organizations provide functions that include, but are not limited to, clinical care, provider practice management, and business operations. Small organizations may not have dedicated IT and security staff to implement cybersecurity practices.[53]
- **Medium to Large** – Generally, these organizations perform critical functions for the healthcare and public health sector. Medium to large organizations typically have dedicated IT resources and staff that address cybersecurity and privacy risks.[54]

1.3.3 Privacy Data Types

The ACA mandates the confidentiality of applicant information, which may only be used for the purposes of, and to the extent necessary to, ensure the efficient operation of the Exchange.[55] ACA AEs and Partner Entities process consumers' and/or beneficiaries' PII (and the PII of their family members, if applicable) during the health insurance coverage eligibility and enrollment process to perform the functions of the Exchange.[56] *ARC-AMPE Volume II* provides the security and privacy framework for ARC-AMPE users to safeguard and protect consumer or beneficiary PII. The safeguards also include those that would facilitate adherence to the HIPAA Security, Privacy, and Breach Notification rules.

In general, privacy interests include an individual's right to decide when and whether to share personal information, how much information to share, and the specific circumstances under which that information can be shared with other parties. Figure 1 depicts what is collectively referred to as "privacy data" in this document: PII,[57] Individually Identifiable Health Information (IIHI),[58] and Protected Health Information (PHI).[59]

[51] ARC-AMPE Volume II includes technical controls that may facilitate adherence to the HIPAA Security, Privacy, and Breach Notification rules. HIPAA CEs and HIPAA BAs may leverage ARC-AMPE Volume II as an informative reference to bolster their security and privacy posture, facilitate adherence to applicable HIPAA requirements, and safeguard consumer or beneficiary PII.

[52] If deemed a Partner Entity, CMS may stipulate the Healthcare Organization implement the required *ARC-AMPE Volume II* controls.

[53] Small healthcare organizations are characterized in Cybersecurity Act of 2015, Section 405(d). More information is available at: https://405d.hhs.gov/Documents/tech-vol1-508.pdf, Technical Volume 1: Cybersecurity Practices for Small Healthcare Organizations.

[54] Medium and large healthcare organizations are characterized in Cybersecurity Act of 2015, Section 405(d). More information is available at: https://405d.hhs.gov/Documents/tech-vol2-508.pdf, Technical Volume 2: Cybersecurity Practices for Medium and Large Healthcare Organizations.

[55] See section 1411(g) of the ACA and 45 CFR §155.260. However, with consumer's consent, PII can also be used for other purposes that comply with section 1411(g)(2)(A) of the ACA. 45 CFR §155.260(a)(1)(iii).

[56] See 45 CFR §155.200.

[57] See Office of Management and Budget (OMB) Memorandum M-17-12 (January 3, 2017).

[58] See 45 CFR §160.103. Individually Identifiable Health Information (IIHI) is a subset of PII.

[59] See 45 CFR §160.103. PHI is a subset of IIHI and PII.

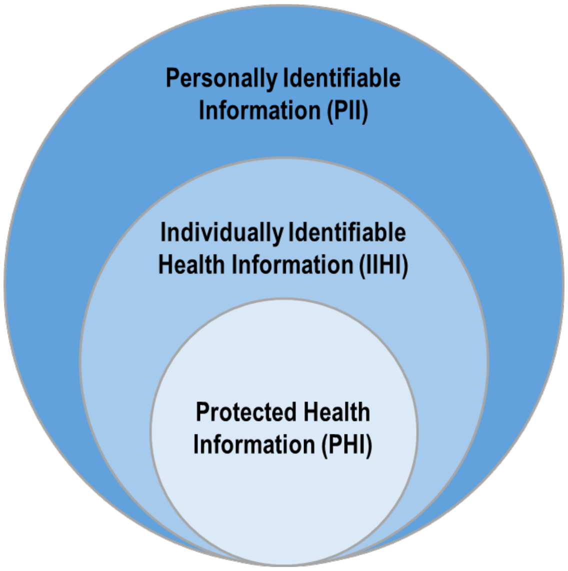

Personally Identifiable Information (PII)
Individually Identifiable Health Information (IIHI)
Protected Health Information (PHI)

Figure 1. Privacy Data Types

Table 1 describes the privacy data types.

Table 1. Privacy Data Type Description

Data Type	Description
Personally Identifiable Information (PII)	• PII is information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.[60] • Can be one of two types: o Direct identifiers – are unique to an individual, e.g., passport number, social security number, or driver's license number.[61] o Indirect identifiers – are not unique to an individual but can identity a person in combination with other indirect identifiers, e.g., uncommon race, ethnicity, extreme age, unusual occupation, and other details.[62] • PII includes Federal Tax Information (FTI). Federal tax returns and return information are confidential to ensure that agencies, bodies, and commissions maintain appropriate safeguards to protect information confidentiality as required in Internal Revenue Code (IRC) §6103.[63]

[60] See Office of Management and Budget (OMB) Memorandum M-17-12 (January 3, 2017).

[61] See NISTIR 8053.

[62] Ibid.

[63] More information on IRS Publication 1075 is available at: https://www.irs.gov/pub/irs-pdf/p1075.pdf.

Data Type	Description
Individually Identifiable Health Information (IIHI)	• IIHI[64] is a subset of health information[65] that includes demographic information collected from an individual that: o Is created or received by a healthcare provider, health plan, employer, or healthcare clearinghouse; o Relates to the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of healthcare to an individual; and o Identifies the individual, or for which there is a reasonable basis to believe that the information can be used to identify the individual.
Protected Health Information (PHI)	• PHI[66] is a subset of IIHI that is held or transmitted by a HIPAA CE or its BA, in any form or media (e.g., electronic, paper, or oral). PHI does not include employment records held by a HIPAA CE in its role as employer, education and certain other records subject to, or defined in, the Family Educational Rights and Privacy Act, or information about a person who has been deceased at least 50 years.

1.4 Audience

All ARC-AMPE users must review *ARC-AMPE Volume I*. ACA AEs and select Partner Entities are required to comply with *ARC-AMPE Volume II*[67] and complete accompanying artifacts to document their compliance with *ARC-AMPE Volume II*.[68] All other organizations may leverage ARC-AMPE as an informative reference to bolster their security and privacy posture, facilitate adherence to applicable HIPAA requirements, and safeguard consumer or beneficiary PII.

1.5 Document Availability and Maintenance

ARC-AMPE Volumes I and *II* will be reviewed and updated as required to ensure the protection of consumer or beneficiary PII against risks and threats. As new cyber and privacy threats or risks emerge, CMS will determine if changes to ARC-AMPE are needed. Other events that may prompt review include updates to federal legislation, HHS regulations, and NIST standards and guidelines (e.g., NIST Special Publication [SP] 800-53 and NIST SP 800-53B).

[64] As defined in 45 CFR §160.103.

[65] Ibid.

[66] Ibid. See also https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.

[67] *ARC-AMPE Volume II* is the System Security and Privacy Plan (SSPP) template with required baseline controls.

[68] Refer to Section 3 for information on which ARC-AMPE users are subject to mandatory compliance with *ARC-AMPE Volume II*.

2. Background

As part of its Exchange oversight responsibility, CMS developed a set of standards for managing security and privacy risks of the Exchanges. Changes to federal laws, agency regulations, NIST standards, and advancements in technology require the continuous update of CMS' security and privacy governance to ensure alignment and relevance.

2.1 ACA Security and Privacy Frameworks

CMS developed guidance and templates, collectively known as the *Minimum Acceptable Risk Standards for Exchanges (MARS-E),* to address the security and privacy mandates of the ACA,[69] and applicable federal laws, HHS regulations, and NIST guidance. *MARS-E* security and privacy control requirements were derived from the *CMS ARS,* which is based on NIST SP 800-53.[70] CMS periodically updated *MARS-E* to reflect the latest security and privacy policies and standards guidance at the national, HHS, and CMS levels. To connect to the Hub, ACA AEs were required to implement the *MARS-E* security and privacy requirements. CMS relied on evidentiary artifacts submitted by an ACA AE to demonstrate implementation of *MARS-E* requirements to make a risk-based decision on whether to approve the ACA AE's Authority to Connect (ATC) to the Hub.[71]

In 2018, CMS established the EDE pathway to facilitate and enhance the Exchange eligibility determination and enrollment processes.[72] In 2019, CMS established the *NEE Governance, Risk Management, and Compliance (GRC) Framework* to accommodate the EDE pathway.[73] NEEs seeking a connection to the Hub were required to demonstrate implementation of the *NEE GRC Framework* security and privacy requirements as evidence of their security and privacy posture.[74] CMS used the evidentiary artifacts submitted by the NEE to demonstrate implementation of *NEE GRC Framework* requirements to make a risk-based decision on whether to grant the NEE's Request to Connect (RTC) to the Hub.

[69] The HHS regulations implementing the security and privacy mandates of the ACA are available at 45 CFR §§155.260 and 155.280.

[70] At the time *MARS-E* was first established, NIST SP 800-53 was on its third revision. At the time of publication of ARC-AMPE, NIST SP 800-53 is on its fifth revision.

[71] Such evidentiary artifacts included, but were not limited to, the System Security and Privacy Plan (SSPP), Penetration Test Results, Plan of Actions and Milestones (POA&M), Privacy Impact Assessment (PIA), Risk Acceptance (RA) Form, Security Assessment Plan (SAP), Security Assessment Report (SAR), Security Assessment Workbook (SAW), and Vulnerability Scans.

[72] EDE is a version of DE that allows consumers to apply for and enroll in individual health insurance coverage through the FFE and SBE-FPs without visiting HealthCare.gov. Approved EDE entities, which include QHP issuers and web-brokers, build and host a version of the HealthCare.gov eligibility application. The application integrates with a suite of FFE application programming interfaces (API) as provided, owned, and maintained by CMS to securely transfer data between the Exchange and the approved EDE Entity's website.

[73] The *CMS ARS* formed the basis for the security and privacy control requirements in the *NEE GRC Framework*. In developing the *NEE GRC Framework*, CMS incorporated the latest guidance of NIST SP 800-171 in the selection and tailoring of controls because CMS Exchange data is processed in non-federal Information systems. CMS also included FedRAMP as part of the selection and tailoring process because most NEE systems are cloud based.

[74] Such evidentiary artifacts included but were not limited to, the System Security and Privacy Plan (SSPP), Penetration Test Results, Plan of Actions and Milestones (POA&M), Risk Acceptance (RA) Form, Security Assessment Plan (SAP), Security Assessment Report (SAR), and Vulnerability Scans.

2.2 Drivers for Change

MARS-E was originally envisioned to apply to the ACA AEs while the *NEE GRC Framework* was intended to address NEEs supporting the ACA functions. Several major updates to federal laws, agency regulations, and NIST standards and guidelines necessitated updating the CMS security and privacy governance, risk management, and compliance frameworks. The required updates presented an opportunity to establish ARC-AMPE, a single, integrated source for security and privacy standards.

ARC-AMPE is the next iteration of security and privacy standards to address the complex business and regulatory environment of the Exchanges.[75] ARC-AMPE incorporates updates to federal laws, agency regulations, and the latest NIST standards and guidelines. ARC-AMPE includes technical controls that may facilitate adherence the HIPAA Security, Privacy, and Breach Notification rules. ARC-AMPE integrates ERM to provide a comprehensive approach to manage risks. ARC-AMPE also accommodates the evolving ACA environment, including additional entities, functions, technology advancements, and legislative changes governing both business functions and security safeguards.

Incorporate Updates to Federal Laws, Agency Regulations, and Security and Privacy Standards

Changes in the federal laws, agency regulations, policies, standards, and guidelines since the inception of the ACA impact CMS functions and business programs. For example, HHS regularly updates its internal policy and guidance on information security programs based on the latest published NIST standards and guidelines. The updates cascade to the security and privacy practices of its Operating Divisions (OpDiv), including CMS. Annual updates to federal regulations implementing the ACA, and new statutes such as the No Surprises Act (NSA) and American Rescue Plan Act (ARPA), also impact CMS' security and privacy practices.

Appendix A. presents more information on the federal, agency, and NIST standards that informed ARC-AMPE.

Integrate ERM

MARS-E and the *NEE GRC Framework* are largely compliance-based frameworks to ensure adherence with all applicable laws, regulations, and standards. A wholly compliance-based framework runs the risk of being reactive and a "checkbox" exercise that may not always consider the broader business context or strategic objectives.

ARC-AMPE supplements the compliance-based approach by integrating ERM, a holistic governance structure that enables identification of technical requirements to mitigate emerging threats and risks. Integrating ERM into ARC-AMPE security and privacy controls allows ARC-AMPE users to adopt a more proactive method to manage enterprise risk, support strategic and risk-informed decision making, improve resource allocation, and protect the organization's assets.

ARC-AMPE aligns business strategy and risk management while balancing compliance with all applicable laws, regulations, and standards. Implementing ARC-AMPE helps users achieve a

[75] *ARC-AMPE* supersedes and replaces *MARS-E* and the *NEE GRC Framework* effective upon publication.

more comprehensive and strategic risk posture. Appendix B. describes how CMS used multiple NIST frameworks to integrate ERM into ARC-AMPE. Appendix C. presents a use case for applying NIST frameworks to identify the ARC-AMPE controls that align business goals with risk management objectives to prioritize cybersecurity and privacy initiatives.

Accommodate New ARC-AMPE Users

Due to the varied types of NEEs supporting the ACA, CMS had to modify the *NEE GRC Framework* to accommodate the nuances of those entities and the data they manage. *ARC-AMPE Volume II* provides a tailorable and flexible security and privacy control set to accommodate potential new ARC-AMPE users as they emerge.

3. Application of ARC-AMPE

CMS requires ACA AEs and select Partner Entities to protect PII in accordance with applicable legal requirements.[76] In furtherance of this, ARC-AMPE establishes guidance for the processing of PII to prevent unauthorized or inappropriate access, use, or disclosure. *ARC-AMPE Volume II* is the tool these entities use to document the implementation of ARC-AMPE security and privacy controls. *ARC-AMPE Volume II* provides an overlay for each ARC-AMPE user, i.e., a tailored control set that aligns and scales with the business, security, and privacy requirements of the ARC-AMPE user type.

3.1 Mandatory Implementation

The mandatory implementation of *ARC-AMPE Volume II* is governed by the applicable security and privacy requirements, legal agreements, and statutory and regulatory authorities. *ARC-AMPE Volume II* must be initiated during the initial stages of the lifecycle process for information systems. Table 2 lists the ARC-AMPE users that must comply with *ARC-AMPE Volume II* by implementing the operational, technical, and physical controls documented in the ARC-AMPE. *ARC-AMPE Volume II* and accompanying evidentiary artifacts should be reviewed by ARC-AMPE users and updated at least annually and when there is a significant change that is likely to substantively affect the security and privacy posture of the IT environment or system.[77] Table 4 provides the list of documents required for submission to CMS.

Table 2. Mandatory ARC-AMPE Implementation

ARC-AMPE User	Role	Description
ACA AE	Federal-facilitated Exchange/Marketplace	• FFE operated by CMS for states that do not have an SBE or SBE-FP
ACA AE	State Medicaid Agency	• State Integrated Eligibility & Enrollment System (IES) connected to FFE through the Hub
ACA AE	State CHIP Agency	• Uses State Medicaid Agency IES to connect to FFE through the Hub
ACA AE	State Basic Health Program (BHP)	• Uses State Medicaid Agency IES to connect to FFE through the Hub
ACA AE	State-based Exchange (SBE)	• Connects state IT environment to the Hub • Downstream entities, such as NEEs or State Medicaid/CHIP Agencies working with SBEs to perform ACA functions must comply with ACA security and privacy provisions

[76] 45 CFR §§155.260 sets forth the privacy and security safeguards for PII.

[77] NIST SP 800-37 Rev. 2 defines a significant change "as a change that is likely to substantively affect the security or privacy posture of a system."

ARC-AMPE User	Role	Description
ACA AE	SBE on the Federal platform (SBE-FP)[78]	• SBE that relies on federal services for some functions, while retaining responsibility for others: o Functions performed by HHS: Eligibility and enrollment o Functions performed by the SBE-FP: Qualified Health Plan (QHP) certification, consumer outreach, and assistance
Partner Entity	Classic Direct Enrollment (Classic DE) Entity	• Operates third-party website to support enrollment activities with or without assistance of an agent broker, directly from their website (web-broker and QHP-issuer)
Partner Entity	Primary Enhanced Direct Enrollment (EDE) Entity	• Develops, designs, and hosts an EDE environment for its own use or for use by others
Partner Entity	Hybrid Issuer Upstream EDE Entity[79] – Implementing Single Sign-on	• Implements single sign-on capability that is out of scope of the approved Primary EDE Entity's IT environment • Can inherit controls from its Primary EDE Entity
Partner Entity	Hybrid Non-Issuer Upstream EDE Entity[80]	• Agents, brokers, or web-brokers that use a primary EDE Entity's EDE environment • Characterized by the presence of additional functionality or systems that modify or add to the Primary EDE Entity's EDE environment beyond minor branding changes or otherwise change the EDE end-user experience
Partner Entity	Service Provider (SP)	• Provides services that enable ACA functions and operations, e.g., income verification and healthcare coverage verification

3.2 Non-Mandatory Implementation

ARC-AMPE users not mandated to implement *ARC-AMPE Volume II* may leverage it as an informative reference to more comprehensively manage their security and privacy posture, facilitate adherence to applicable HIPAA requirements, and safeguard consumer or beneficiary PII. It is strongly recommended that the ARC-AMPE users listed in Table 3 implement the operational, technical, and physical controls documented in the *ARC-AMPE Volume II* overlay as applicable to the ARC-AMPE user type.

[78] See 45 CFR §155.106(c).

[79] Hybrid Issuer Upstream EDE Entity is defined in the EDE Business Agreement.

[80] Ibid.

Table 3. Non-Mandatory ARC-AMPE Implementation

ARC-AMPE User	Role	Description
Partner Entity	Hybrid Issuer Upstream EDE Entity – Excluding Those Implementing Single Sign-on	• Uses an EDE environment provided by a Primary EDE Entity • Implements, or has a Primary EDE Entity implement on its behalf, additional functionality or systems to the primary EDE Entity's EDE environment beyond minor branding changes or QHP display changes
Partner Entity	Upstream EDE – White-Label User	• Uses an EDE environment provided by a Primary EDE Entity but does not implement any additional functionality or systems other than minor branding changes
Partner Entity	Agent/Broker Entity (ABE)	• A collective term for Agents, Brokers, and Agent or Broker Entities that have been licensed by the state and registered with the Exchange • Assists consumers with enrollment in an QHP
Partner Entity	Service Provider	• Performs non-ACA functions, e.g., dispute resolution
State Healthcare Agency	State Medicaid Agency and/or State Health and Human Services Agency	• Performs non-ACA functions, e.g., support Medicaid Management Information Systems (MMIS) operations • Is not an ACA AE • May be considered a HIPAA CE or HIPAA BA
Small Healthcare Organization	Small Healthcare Organization	• Generally, a small organization that does not have a dedicated IT and security staff • Accesses consumer or beneficiary PII • Supports other healthcare programs such as Medicaid/CHIP or state healthcare programs • Performs non-ACA functions • May be a HIPAA CE or HIPAA BA
Medium/Large Healthcare Organization	Medium/Large Healthcare Organization	• Generally, have dedicated IT departments and likely have dedicated cybersecurity staff that address cybersecurity threats • Accesses consumer or beneficiary PII • Supports other healthcare programs such as Medicaid/CHIP or state healthcare programs • Performs non-ACA functions • May be a HIPAA CE or HIPAA BA

4. Reporting Requirements for Mandatory Implementation

4.1 Authorization

ACA AEs and select Partner Entities listed in Table 2 must submit the applicable evidentiary artifacts listed in Table 4 to demonstrate the security and privacy risk posture of the entity's information system. CMS reviews the evidentiary artifacts for completeness, accuracy, and compliance with *ARC-AMPE Volume II* control requirements. CMS also verifies the entity has taken the necessary steps to resolve or mitigate all outstanding security and privacy findings, risks, vulnerabilities, or issues. CMS then makes a risk-informed decision on whether to grant the connection to the Hub.

Authorization of the entity's connection to the Hub is documented in the Interconnection Security Agreement (ISA). The ISA establishes the Authority to Connect (ATC) for AEs and the Request to Connect (RTC) for NEEs. Depending on the types of data processed, the entity may also be required to enter into other legal agreements.[81]

Table 4. Non-Exhaustive List of ARC-AMPE Artifacts

Non-Exhaustive List of ARC-AMPE Artifacts
ARC-AMPE Volume II (System Security and Privacy Plan [SSPP])[82]
Change Notification (CN) Form
Computer Matching Agreement (CMA)
Data Use Agreement (DUA)
Information Exchange Agreement (IEA)
Information System Risk Assessment (ISRA)
Interconnection Security Agreement (ISA)
Memorandum of Understanding / Agreement (MOU / MOA)
Penetration Test Results[83]
Plan of Actions and Milestones (POA&M)[84]
Privacy Impact Assessment (PIA)
Risk Acceptance (RA) Form
Security Assessment Plan (SAP)
Security Assessment Report (SAR)
Security Assessment Workbook (SAW)[85]

[81] Other legal agreements may include but are not limited to a Business Agreement, Data Use Agreement, Information Exchange Agreement, and Computer Matching Agreement.

[82] In addition to the assigned controls, each entity must perform an assessment of its own environment to determine what additional controls are needed.

[83] For Penetration Test Results, follow the submission timelines provided in each ARC-AMPE user-type Information System Continuous Monitoring (ISCM) Guide.

[84] For POA&Ms, follow the submission timelines provided in each ARC-AMPE user-type ISCM Guide.

[85] The SAW is required for ACA AEs only.

Non-Exhaustive List of ARC-AMPE Artifacts
Security Impact Assessment (SIA)
Vulnerability Scans[86]

ARC-AMPE Volume II and accompanying evidentiary artifacts are released in template format. Select ARC-AMPE users must submit artifacts based on the security and privacy requirements and schedule.[87]

4.2 Information System Continuous Monitoring

Information security and privacy continuous monitoring (ISCM) is a dynamic process that must be effectively and proactively managed to support organizational risk management decisions. ISCM enables ARC-AMPE users to identify and address new vulnerabilities, evolving threats, and changes in enterprise architecture and operational environments, including hardware or software. It also addresses risk associated with the processing of PII.

Once CMS approves an ARC-AMPE user's authorization, the user must maintain compliance with *ARC-AMPE Volume II* controls. To maintain the information security and privacy risk posture of an IT system, ARC-AMPE users must monitor and regularly assess their security and privacy controls.[88] ISCM activities must commence immediately upon authorization approval. The ARC-AMPE user must demonstrate the effectiveness of its continuous monitoring program through evidentiary information. After an authorization is approved, the ARC-AMPE user and its auditor must submit this evidence to CMS in accordance with the submission timelines provided in each ARC-AMPE user-type ISCM Guide. CMS relies on these evidentiary deliverables to gain operational visibility into the ARC-AMPE users' environment. Through ongoing assessment and authorization, CMS can detect changes in the security and privacy posture of an ARC-AMPE user's IT system, which is crucial for making informed, risk-based decisions within the CMS environment.

[86] For Vulnerability Scans, follow the submission timelines provided in each ARC-AMPE user-type ISCM Guide.

[87] ACA AEs must comply with the latest *Timelines and Artifacts* document.

[88] ACA AEs must comply with the latest *Information Security and Privacy Continuous Monitoring (ISCM) Guide for Administering Entity (AE) Systems*. NEEs must comply with the latest the *NEE Information Security and Privacy Continuous Monitoring (ISCM) Strategy Guide.*

Appendix A. Updated Laws, Regulations, Policies, and NIST Standards and Guidelines

ARC-AMPE addressed the following changes in federal laws, agency regulations, agency policies, and National Institute of Standards and Technology (NIST) standards and guidelines.

A.1 Laws, Regulations, and Policies

The updated federal laws, agency regulations, and agency policies include:

- ***HHS Information Systems Security and Privacy Policy (IS2P)***, which provides policy guidance to information security programs of Department of Health and Human Services (HHS) Operating Divisions (OpDiv). The Federal Information Security Modernization Act (FISMA) compliance requirements and updates to NIST guidance drove many of these changes to the IS2P.
- ***CMS Information Systems Security & Privacy Policy (IS2P2)***, which provides the Agency's framework for protecting and controlling access to CMS information and information systems, also impacts CMS' security and privacy practices. HHS IS2P updates drove changes to the IS2P2.
- **No Surprises Act (NSA),** which was signed into law on December 27, 2020, as part of the Consolidated Appropriations Act of 2021 (CAA). The passage of the CAA established protections for consumers related to surprise billing and transparency in healthcare. The NSA introduces new ACA partners to CMS security and privacy oversight.[89]
- **21st Century Cures Act**, which resulted in the Trusted Exchange Framework and the Common Agreement (TEFCA) for Health Information Networks created by the HHS Office of the National Coordinator for Health Information Technology (ONC).[90]
- **Cybersecurity Act of 2015 (CSA), Section 405(d), Aligning Health Care Industry Security Approaches**, directs the HHS Secretary to establish, in collaboration with the Secretary of Homeland Security, healthcare industry stakeholders, the Director of the NIST, and any federal entity or non-federal entity the Secretary determines appropriate, a common set of voluntary, consensus-based, and industry-led guidelines, best practices, methodologies, procedures, and processes in order to strengthen the Healthcare and Public Health (HPH) sector's cybersecurity posture against cyber threats.[91]
- **Health Insurance Portability and Accountability Act, (HIPAA)**, is a federal law enacted in 1996 that protects patients' personal health information (PHI) by regulating its use, disclosure, and security. HIPAA requires healthcare providers, employees, contractors, students, and any individual with access to PHI to acknowledge their

[89] https://www.cms.gov/nosurprises.

[90] https://www.healthit.gov/topic/interoperability/policy/trusted-exchange-framework-and-common-agreement-tefca.

[91] https://405d.hhs.gov/.

understanding of HIPAA regulations and agree to maintain the confidentiality and security of PHI.[92]

- **Health Information Technology for Economic and Clinical Health (HITECH Act)**, which requires the HHS to consider whether a covered entity or business associate has adequately demonstrated recognized security practices. The HITECH Amendment provides that "recognized security practices" (RSP) include: (1) standards, guidelines, best practices, methodologies, procedures, and processes developed under section 2(c)(15) of the National Institute of Standards and Technology Act; (2) the approaches promulgated under section 405(d) of the Cybersecurity Act of 2015; and (3) other programs and processes that address cybersecurity and that are developed, recognized, or promulgated through regulations under other statutory authorities.[93]
- **HHS Notice of Benefit and Payment Parameters**, which are annual rulemakings that include, among other things, requirement updates for agents, brokers, web-brokers, and Partner Entities assisting consumers in the eligibility and enrollment functions.
- **American Rescue Plan Act (ARPA)**, which made premium tax credits available to eligible taxpayers with household income above 400 percent of the Federal Poverty Line (FPL) and capped how much of household income the family will pay toward the premiums for a benchmark plan at 8.5 percent before premium tax credits apply. The ARPA also reduced the percentage of household income eligible taxpayers at all income levels are expected to contribute to their monthly premiums for a benchmark plan before premium tax credits apply.
- **Inflation Reduction Act (IRA)**, which extended the ARPA premium tax credit through the 2025 plan year.

A.2 NIST Standards and Guidelines

The updated NIST standards and guidelines include:

- **NIST SP 800-53, Rev. 5, *Security and Privacy Controls for Information Systems and Organizations***. Revision 5 of NIST Special Publication (SP) 800-53 impacted many of the source documents of the ACA security and privacy frameworks and is among the major drivers for change. NIST SP 800-53 Rev. 5 is the fundamental source document for *CMS Acceptable Risk Safeguards (ARS)*, which is the source document for the *ARC-AMPE Volume II*, and for the Federal Risk and Authorization Management Program (FedRAMP).[94] NIST SP 800-53 controls are flexible, customizable, and implemented as part of an organization-wide process to manage risk.

  The latest NIST SP 800-53 Rev. 5 control catalog was updated to reflect safeguards and protective measures that can support both security and privacy needs and manage risk. The updated consolidated catalog also contains new control families, including one specific to Personally Identifiable Information (PII) processing and transparency.

[92] https://www.hhs.gov/hipaa/index.html

[93] https://www.federalregister.gov/documents/2022/04/06/2022-07210/considerations-for-implementing-the-health-information-technology-for-economic-and-clinical-health.

[94] FedRAMP issues guidance for systems operating in the cloud environment.

NIST SP 800-53 Rev. 5 includes guidance on the concept of trustworthiness and the fundamental concepts of functionality (i.e., security and privacy features, functions, and mechanisms implemented within an organization) and assurance[95] that affect trustworthiness and are addressed by security and privacy controls.

- **NIST SP 800-53B, *Control Baselines for Information Systems and Organizations***. NIST SP 800-53B, an accompanying document to NIST SP 800-53 Rev. 5, provides security (Low, Moderate, and High) and privacy control baselines for the federal government. The control baselines provide a starting point for organizations in the security and privacy control selection process. In developing the ARC-AMPE, CMS drew on the tailoring guidance in NIST SP 800-53B to help guide and inform the control selection process. CMS referred to this publication for the starting Moderate baseline control set and the Privacy Control Baseline. CMS also relied on NIST SP 800-53B guidance to help inform tailoring control baselines to protect critical and essential operations to reflect CMS-specific safeguarding needs.
- **NIST SP 800-171, Rev. 3, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations***. This publication provides agencies with recommended security requirements for protecting the confidentiality of Controlled Unclassified Information (CUI)[96] when the information is resident in nonfederal systems and organizations. The requirements in NIST SP 800-171 Rev. 3 apply to all components of nonfederal systems and organizations that process, store, and/or transmit CUI, or that provide protection for such components. The security requirements are intended for use by federal agencies in contractual vehicles or other agreements established between those agencies and nonfederal organizations.

  The nature of the ACA enables maintenance of ACA consumer data in a nonfederal information technology environment. This ACA consumer data, which is PII and a category of CUI, must be protected appropriately. The NIST SP 800-171 safeguards provide the security requirements for protecting the confidentiality of this CUI.

[95] For more information on functionality and assurance, refer to Section 2.5 “Trustworthiness and Assurance” in NIST SP 800-53, Revision 5.

[96] Controlled Unclassified Information is defined as “information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulations, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls.” https://www.archives.gov/cui/registry/cui-glossary.html#C

Appendix B. Enterprise Risk Management

Effective Enterprise Risk Management (ERM) prioritizes business functions, budget, and priorities in concert with cybersecurity requirements, risk posture, and risk tolerance. It also aligns resources (e.g., budget) and capital planning with organizational priorities and unaddressed gaps or initiatives. ERM is a holistic governance structure that enables identification of technical requirements to mitigate emerging threats and risks. The Centers for Medicare & Medicaid Services (CMS) incorporated ERM into ARC-AMPE by following National Institute of Standards and Technology (NIST) frameworks[97] (i.e., *Cybersecurity Framework* [CSF],[98] *Privacy Framework*,[99] and *Risk Management Framework* [RMF]) and guidance for integrating cybersecurity and ERM.[100]

B.1 Cybersecurity Framework

The NIST CSF[101] provides flexible, risk-focused, and voluntary guidance based on existing standards, guidelines, and practices to help organizations better understand, manage, reduce, and communicate cybersecurity risks. As a strategic framework, the CSF enables organizations and agencies—regardless of size, degree of cybersecurity risk, or cybersecurity sophistication—to apply the principles and best practices of risk management to improve security and resilience.

CMS expanded the ARC-AMPE risk management methodology to include the CSF and its strategic cybersecurity risk management guidance. CMS considered and was informed by the CSF Informative References mapping in developing the *ARC-AMPE Volume II*. Appendix C. provides an implementation use case example developed by CMS to demonstrate how ARC-AMPE users can use the NIST Cybersecurity Framework or Privacy Profile tools to manage cybersecurity and privacy risks. Appendix also articulates how to implement NIST Profiles to make strategic and resource-informed decisions when implementing required *ARC-AMPE Volume II*.

[97] The Agency acknowledges NIST for the use of Figure 2 and Figure 3 in this appendix.

[98] CMS used the NIST CSF version 1.1, which was the latest version available when CMS created the *ARC-AMPE*. ARC-AMPE users should rely on the most current NIST CSF, version 2.0 (February 26, 2024), which is available at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf.

[99] Information about the NIST Privacy Framework is available at: https://www.nist.gov/privacy-framework.

[100] NIST IR 8286 series is available at: https://csrc.nist.gov/pubs/ir/8286/final#pubs-abstract-header.

[101] Originally, the NIST CSF was designed for organizations that are part of the U.S. critical infrastructure under Executive Order (EO) 13636, *Improving Critical Infrastructure Cybersecurity.* Organizations in the private and public sectors use the CSF to manage cybersecurity risk. In 2017, EO 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, broadened use of the CSF beyond U.S. critical infrastructure and required that U.S. federal government agencies use the NIST CSF to manage cybersecurity risks.

B.2 Privacy Framework

An essential responsibility of the Exchange and all its business partners is protecting and ensuring the privacy and security of the Exchange information, common enrollment information, and associated information systems. CMS integrated the Privacy Framework into the ARC-AMPE to comply with data protection and privacy laws and manage privacy risk to the individuals participating in the Exchange. *ARC-AMPE Volume II* were mapped to and validated against existing laws, regulations, and policies to ensure alignment.

The Privacy Framework considers privacy events as potential problems individuals could experience. Figure 2[102] depicts the overlapping nature of security and privacy risks.

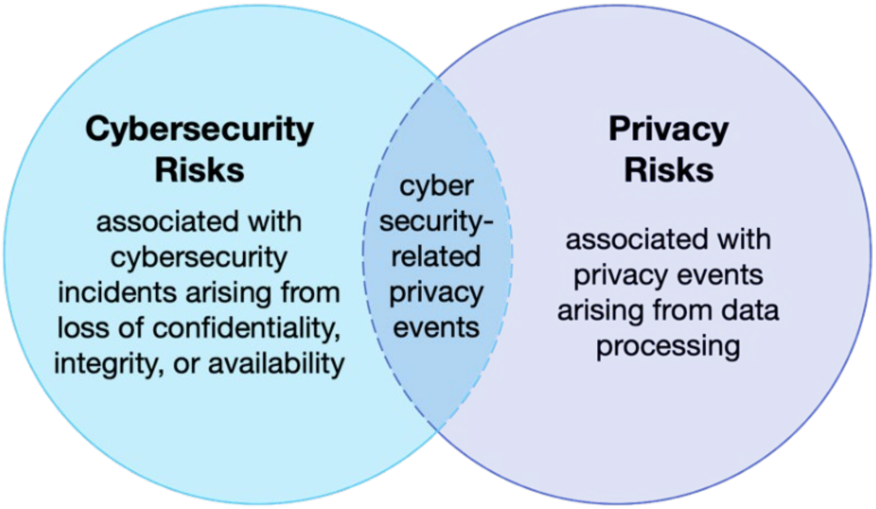

Cybersecurity Risks
associated with cybersecurity incidents arising from loss of confidentiality, integrity, or availability
cyber security-related privacy events
Privacy Risks
associated with privacy events arising from data processing

Figure 2. Cybersecurity and Privacy Risk Relationship

B.3 Risk Management Framework (NIST SP 800-37)

The NIST RMF addresses organizations' security and privacy concerns related to the design, development, implementation, operation, maintenance, and disposal of information systems and the environments in which those systems operate. As depicted in Figure 3, the RMF comprises system-level steps and activities with control sets to safeguard a system, its assets, and environment of operation.[103]

[102] More information is available at: https://www.nist.gov/privacy-framework/getting-started-0.

[103] NIST SP 800-37, Revision 2, Section 2.2 "Risk Management Framework Steps and Structure." For more information on the RMF steps, refer to Chapter 3, "The Process."

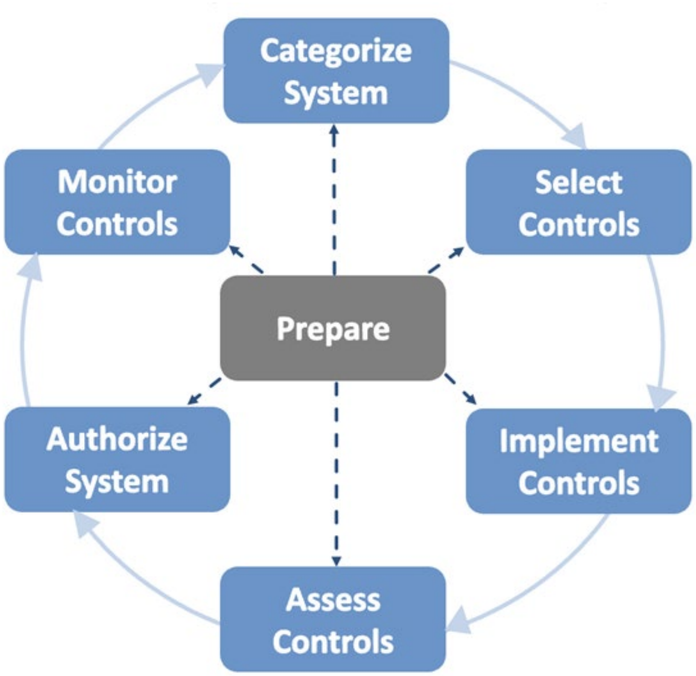


Figure 3. NIST Risk Management Framework Steps

Control sets typically reflect impacts that result from a loss of a system's security objective (i.e., confidentiality, integrity, or availability) and must be tailored to reflect strategic risk management priorities based on an understanding of organizational priorities and how a system supports those priorities. The RMF methodology guided development of the ARC-AMPE.

Appendix C. ARC-AMPE Application of NIST Risk Management Framework

In its role to guide and provide oversight for the Exchanges, the Centers for Medicare & Medicaid Services (CMS) used the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF)[104] methodology to create the standards to manage security and privacy risk. Following the steps of the NIST RMF methodology, CMS established the ARC-AMPE system-level control sets based on the NIST Moderate baseline (NIST SP 800-53B) and tailored the baseline as appropriate using the controls in NIST SP 800-53 Rev. 5 Chapter 3. Table 5 describes NIST RMF activities and responsible ARC-AMPE parties.

Table 5. ARC-AMPE Application of NIST Risk Management Framework

NIST RMF Activity	Description	ARC-AMPE Responsible Party
Prepare	Essential activities to **prepare** the organization to manage security and privacy risks	ARC-AMPE User
Categorize	**Categorize** the system and information processed, stored, and transmitted based on an impact analysis	CMS
Select	**Select** the set of NIST SP 800-53 controls to protect the system based on risk assessment(s)	CMS
Implement	**Implement** the controls and document how controls are deployed	ARC-AMPE User
Assess	**Assess** to determine if the controls are in place, operating as intended, and producing the desired results	ARC-AMPE User
Authorize	Senior official makes a risk-based decision to **authorize** the system (to operate)	CMS
Monitor	Continuously **monitor** control implementation and risks to the system	ARC-AMPE User

C.1 Categorize the System and Information

Federal Information Processing Standards (FIPS) Publication 199, which provides the standards for security categorization of federal information and information systems, requires agencies to determine a single overall impact level (high-water mark) of low, moderate, or high for the information system. This high-water mark is the most stringent impact level based on the potential adverse effect of the loss of a security objective (i.e., confidentiality, integrity, or availability) on organizational operations, organizational assets, or individuals.

CMS categorized the information systems supporting the ACA functions as Moderate based on:

[104] More information can be found in NIST SP 800-37 Rev. 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy,* available at: https://csrc.nist.gov/pubs/sp/800/37/r2/final.

- ACA AE and Partner Entities' processing of Personally Identifiable Information (PII), which could result in serious adverse effects on ACA operations should there be a loss of a security objective; and
- NIST SP 800-171 security requirements for protecting PII, which is a type of Controlled Unclassified Information (CUI).[105]

C.2 Select and Tailor Security and Privacy Control Sets

CMS used NIST SP 800-53B[106] to inform the ARC-AMPE control selection process. This publication contains the control baselines that an organization uses to start the security and privacy control selection process.

To tailor the controls in *ARC-AMPE Volume II*, CMS analyzed the business program objectives and outcomes of key ACA functions and operations[107] while balancing information security requirements and risks unique to CMS systems. CMS also considered the data accessed and/or used by these functions and operations, including consumer or beneficiary PII, and how to protect this information in non-federal systems and organizations.[108] Another control selection consideration was that IT environments are increasingly implemented in the cloud.

To refine the control selection and tailoring, CMS collaborated with program managers from the ACA AEs, NEEs, EDEs, and Medicaid as well as external stakeholders such as state representatives. *ARC-AMPE Volume II* incorporates key standards and processes to support governance, risk management, and compliance with the federal laws and regulations governing security and privacy.[109]

C.3 Implement and Assess Appropriate Control Sets

ARC-AMPE Volume II provides the minimum security and privacy controls for ARC-AMPE users. The ARC-AMPE controls must be implemented by ACA AEs and select Partner Entities.[110] Depending on the types of data processed, an ARC-AMPE users' information systems may be required to meet additional security control requirements as mandated by specific sources, whether federal, state, or local laws or regulations. An entity may also choose to

[105] Controlled Unclassified Information is defined as "information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulations, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls." https://www.archives.gov/cui/registry/cui-glossary.html#C

[106] More information on NIST SP 800-53B is available at: https://csrc.nist.gov/pubs/sp/800/53/b/upd1/final.

[107] The NIST Cybersecurity Framework and the Privacy Framework were consulted to analyze the business objectives and outcomes of key business operations.

[108] More information on protecting PII in non-federal systems can be found in NIST SP 800-171 Rev. 3, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations* and available at: https://csrc.nist.gov/pubs/sp/800/171/r3/final.

[109] Pairing the RMF with the NIST CSF and Privacy Framework enabled CMS to identify and prioritize RMF-related cybersecurity activities and outcomes that are necessary to safeguard Exchange data. Appendix C provides more information about these NIST frameworks.

[110] Refer to Section 3 for the list of entities that must implement controls in *ARC-AMPE Volume II*.

implement more stringent control parameters[111] or additional controls[112] for more rigorous protection. Entities are obligated to comply with the requirements of any other applicable laws and regulations that apply to them (e.g., Titles XVIII and XIX for Medicaid / CHIP agencies and 26 U.S.C. §6103, Safeguards for Protecting Federal Tax Returns and Return Information).[113]

CMS requires ACA AEs and select Partner Entities to demonstrate their implementation of the controls in *ARC-AMPE Volume II*. They may be required to retain an independent third-party auditor to assess the implementation of the controls in *ARC-AMPE Volume II*. The auditor would engage with the ARC-AMPE user and use CMS-designated guidance and templates to report assessment outcomes to CMS.

C.4 Authorize Connection

Upon CMS' acceptance of an ARC-AMPE user's applicable evidentiary artifacts demonstrating the security and privacy risk posture of the entity's information system, CMS makes a risk-informed decision on whether to grant the connection to the Hub. CMS bases the decision on the agency's review of the evidentiary artifacts for completeness, accuracy, and compliance with ACA security and privacy requirements. CMS also verifies the entity has taken the necessary steps to resolve or mitigate all outstanding security and privacy findings, risks, vulnerabilities, or issues. Authorization of the entity's connection to the Hub is documented in the Interconnection Security Agreement (ISA). The ISA establishes the ATC for AEs and the RTC for NEEs. Depending on the types of data processed, the entity may also be required to enter into other legal agreements.[114]

C.5 Monitor Control Implementation and Risks

Information System Continuous Monitoring (ISCM) and its associated activities provide a mechanism to maintain awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. ISCM provides continuous visibility into the security and privacy risk posture of an organization's systems rather than single point-in-time assessments, enabling timely detection and response to any changes in the system's security state.

ACA AEs and select Partner Entities connected to the Hub must continuously assess their implementation of the *ARC-AMPE Volume II* controls to ensure the entity maintains a risk posture that is acceptable with ARC-AMPE standards for access to the Hub. CMS requires ARC-AMPE users to provide evidentiary artifacts and the results of ISCM activities based on the specific security and privacy requirements for the ARC-AMPE user.

[111] When assigning these parameter values, organizations should consider regulations, statutes, administrative rules, or other similar types of guidance and requirements for safeguarding their systems and information.

[112] Organizations cannot remove or reduce the controls included within the CMS ARC-AMPE baseline; however, organizations may add controls to the CMS ARC-AMPE baseline, provided those controls do not conflict with or create less stringent standards than the baseline. Any added controls should be the result of a risk-informed decision based on specific mission and business functions, environments of operation, threats and vulnerabilities that can affect their systems, and any other conditions or situations that can impact their organization.

[113] HIPAA Business Associates are required to comply with the specific terms of their Business Associate Agreement, which may include more stringent controls than those established in the HIPAA Rules.

[114] Other legal agreements may include but are not limited to a Business Agreement, Data Use Agreement, Information Exchange Agreement, and Computer Matching Agreement.

Appendix D. Use Case for Applying NIST Frameworks

This appendix provides a use case that demonstrates how the Centers for Medicare & Medicaid Services (CMS) applied the *National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) v1.1*[115] and *NIST Privacy Framework v1.0* to develop a notional ACA Administering Entity (AE) CSF Profile and ACA AE Privacy Framework Profile. The profile identifies ARC-AMPE controls that align business goals with risk management objectives to prioritize cybersecurity and privacy initiatives. The CMS-developed ACA AE CSF Profile is an example of how the ARC-AMPE users can use the NIST CSF and Privacy Framework to make strategic and resource-informed decisions when implementing the *ARC-AMPE Volume II*.

D.1 Background

Application of the NIST CSF and NIST Privacy Framework can include creating Profiles, which communicate the alignment of enterprise priorities and cybersecurity or privacy risk throughout an organization. A Profile is a flexible, customizable tool to help understand, prioritize, and assess progress of cybersecurity outcomes that are reasonable and appropriate to balance the organization's risk posture with its business requirements, risk tolerance, and resources.[116]

Organizations use Profiles to describe their current and/or target cybersecurity and privacy posture and determine cybersecurity priorities. An entity can use the ACA AE CSF and Privacy Framework Profiles to assess its progress toward achieving its desired target cybersecurity and privacy posture and communicate those outcomes among stakeholders.[117] Profiles can play a role in aiding cybersecurity and privacy risk management, strategic communications, and resource allocation.

D.2 Use Case

CMS developed this use case of a notional ACA AE CSF Profile and an ACA AE Privacy Framework Profile to demonstrate how a state can use the NIST CSF and Privacy Framework in their organization.

[115] CMS used NIST CSF version 1.1, which was the latest version available when CMS created the *ARC-AMPE*. ARC-AMPE users should employ the most current NIST CSF, version 2.0 (February 26, 2024), which is available at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf, and the most current Privacy Framework.

[116] Entities are encouraged to review the NIST CSF at https://www.nist.gov/cyberframework/csf-11-archive and the NIST Privacy Framework at https://www.nist.gov/privacy-framework for additional information and resources for safeguarding individuals' privacy.

[117] More information on the NIST CSF is available at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf. A quick-start guide for creating and using organizational profiles is available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1301.pdf.

D.2.1 ACA AE CSF Profile

CMS employed the following process to develop the ACA AE CSF Profile:

- Define the pillars or top-level business activities of the ACA AE.
- Establish the cybersecurity outcomes prioritization methodology.
- Determine priority levels for the CSF Profile Subcategories.

D.2.1.1 Define Pillars

Pillars are those guiding principles, with potential cybersecurity or privacy impact, that can support an organization’s ability to accomplish its primary mission. Pillars may include customer-facing activities, back-office operations, supply chain support, research and development, manufacturing, and human resources.

CMS drafted seven ACA AE Pillars based on mission statements consistent across ACA AEs, CMS healthcare subject matter expertise, and ACA AE stakeholder input. The Agency validated the ACA AE Pillars and priority order in working sessions with ACA AE representatives. The resulting prioritized Pillars represent overall business goals and cybersecurity objectives for ACA AEs.

Table 6 presents the ACA AE Pillars for this use case, ordered according to the relative importance to the enterprise and the risk each Pillar poses to an ACA AE operating environment if the Pillar were compromised. Although the table reflects a notional priority order specific to ACA AEs, this set of Pillars reflects the overall ARC-AMPE environment. ACA AEs can adopt and adapt the priority order of the Pillars or determine their applicability to their respective organizations.

Table 6. ACA AE Pillars

Number	Pillar Description
1	Engage with and empower the consumer to make informed healthcare and coverage decisions
2	Provide a seamless experience by effectively managing end-to-end operations for partners/stakeholders throughout the health coverage enrollment lifecycle
3	Foster trust and ensure transparency and accountability in healthcare program operations and processes
4	Promote and enable accessibility and availability of health coverage products and/or services to customers to meet the needs of a diverse population
5	Maintain compliance with federal laws, agency regulations, policies, and agreements
6	Drive innovation to overcome health system challenges
7	Promote simple, affordable product options that facilitates continuity of care

D.2.1.2 Establish the Prioritization Methodology for Cybersecurity Outcomes

Pillars provide the necessary context for managing an entity's cybersecurity risk and guiding cybersecurity activities to accomplish a specific mission need. CMS reviewed the ACA AE's cybersecurity risks against enterprise business functions to develop a list of CSF Subcategories grouped by priority levels. Entities should consider all CSF Subcategories when they develop these groupings. Entities can use the ACA AE CSF Profile's prioritized Subcategories to refine their implementation of cybersecurity and privacy controls.

CMS holistically evaluated the seven prioritized Pillars in Table 6 by considering the criticality of the Subcategories in supporting all Pillars and an individual Pillar's priority. CMS applied this analysis to determine relevant priority cybersecurity outcomes for ACA AEs and created a list of CSF v1.1 Subcategories by priority level. Subcategories have three priority levels:

- **High Priority –** This level identifies the most critical Subcategories that support a Pillar. Entities should address high-priority Subcategories most immediately, given available resources.
- **Moderate Priority –** This level applies to a Subcategory that should be implemented next after any High Priority Subcategory. At this level, a Pillar depends on the Subcategory, but the dependency is not as critical as a High Priority Subcategory. (In certain contexts or environments, this level may become a higher priority.)
- **Other Priority –** This level of Subcategory may not require the urgency of Moderate or High Priority Subcategories but is nevertheless important to the overall cybersecurity of the Pillar(s). This level does not equate to low priority.

ACA AEs should evaluate all Categories and Subcategories to identify, prioritize, and address their specific cybersecurity needs and risk tolerance. Table 7 and Table 8 present the High and Moderate NIST CSF Subcategory priorities applied respectively for the ACA AE use case.[118] CMS mapped the Subcategories to the corresponding related controls in NIST SP 800-53 Rev. 5.[119]

D.2.1.3 Determine Priority Levels for CSF Profile Subcategory

Applying the Cybersecurity Priority outcomes methodology, CMS grouped the Subcategories in Table 7 as High Priority and Table 8 as Moderate Priority.

As shown, most of the Subcategories prioritized as High and Moderate are from the Identify and Protect Functions. The Subcategories in these functions were considered the most critical to support the ACA AE Use Case Pillars and identify critical functions and dependencies, establish clear governance processes, and protect the entity's assets and data.

Each entity should consider its own business requirements, goals, and priorities when using the ACA AE Use Case. Entities may decide that within their cybersecurity risk management program, there may be Other Priority Subcategories that should be elevated in priority. A CSF Subcategory's priority can inform Profile stakeholders on decisions and resource needs to achieve cybersecurity risk management objectives and Pillars. *ARC-AMPE Volume II*

[118] CMS adapted the NIST CSF v. 1.1 tables by sorting according to ACA AE Use Case prioritization.

[119] NIST CSF v1.1 mapping to NIST SP 800-53 Rev 5 controls are available at: "Mappings: Cybersecurity Framework and Privacy Framework to Revision 5," https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final.

implementers can use prioritized Subcategories to determine which cybersecurity activities and outcomes are most important and guide efforts to select, tailor, implement, and monitor controls at the system/program level given limited resources.

Table 7. High Priority Subcategories for the ACA AE Use Case

Function	NIST CSF Subcategory	NIST SP 800-53 Rev. 5 Controls
IDENTIFY	**ID.BE-4:** Dependencies and critical functions for delivery of critical services are established	CP-2, CP-8, PE-9, PE-11, PM-8, RA-9, SA-20, SR-2
IDENTIFY	**ID.BE-3:** Priorities for organizational mission, objectives, and activities are established and communicated	PM-11
IDENTIFY	**ID.BE-5:** Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	CP-2, CP-11, RA-9, SA-8, SA-20
IDENTIFY	**ID.BE-1:** The organization's role in the supply chain is identified and communicated	SR-1, SR-3
PROTECT	**PR.DS-2:** Data-in-transit is protected	SC-8, SC-11
IDENTIFY	**ID.GV-1:** Organizational information cybersecurity policy is established and communicated	-1 controls from all security control families
IDENTIFY	**ID.GV-3:** Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	-1 controls from all security control families
IDENTIFY	**ID.GV-2:** Cybersecurity roles & responsibilities are coordinated and aligned with internal roles and external partners	PS-7, PS-9, PM-1, PM-2, PM-29
IDENTIFY	**ID.GV-4:** Governance and risk management processes address cybersecurity risks	PM-3, PM-7, PM-9, PM-10, PM-11, PM-28, RA-1, RA-2, RA-3, SA-2
DETECT	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed	AC-4, CA-3, CM-2, SC-16, SI-4
IDENTIFY	**ID.BE-2:** The organization's place in critical infrastructure and its industry sector is identified and communicated	PM-8
PROTECT	**PR.DS-1:** Data-at-rest is protected	MP-2, MP-3, MP-4, MP-5, MP-6, MP-7, MP-8, SC-28
PROTECT	**PR.DS-5:** Protections against data leaks are implemented	AC-4, AC-5, AC-6, AU-13, PE-19, PS-6, SC-7, SI-4
PROTECT	**PR.DS-3:** Assets are formally managed throughout removal, transfers, and disposition	CM-8, MP-6, PE-16, PE-20
PROTECT	**PR.DS-4:** Adequate capacity to ensure availability is maintained	AU-4, CP-2, PE-11, SC-5
PROTECT	**PR.DS-6:** Integrity checking mechanisms are used to verify software, firmware, and information integrity	SI-7, SI-10

Function	NIST CSF Subcategory	NIST SP 800-53 Rev. 5 Controls
DETECT	**DE.AE-4:** Impact of events is determined	CP-2, IR-4, RA-3, SI-4
IDENTIFY	**ID.AM-3:** Organizational communication and data flows are mapped	AC-4, CA-3, CA-9, PL-8, SA-17
DETECT	**DE.AE-2:** Detected events are analyzed to understand attack targets and methods	AU-6, CA-7, RA-5, IR-4, SI-4
DETECT	**DE.AE-5:** Incident alert thresholds are established	IR-4, IR-5, IR-8
PROTECT	**PR.AC-1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices users, and processes	IA-1, IA-2, IA-3, IA-4, IA-5, IA-7, IA-8, IA-9, IA-10, IA-11, IA-12

Table 8. Moderate Priority Subcategories for the ACA AE Use Case

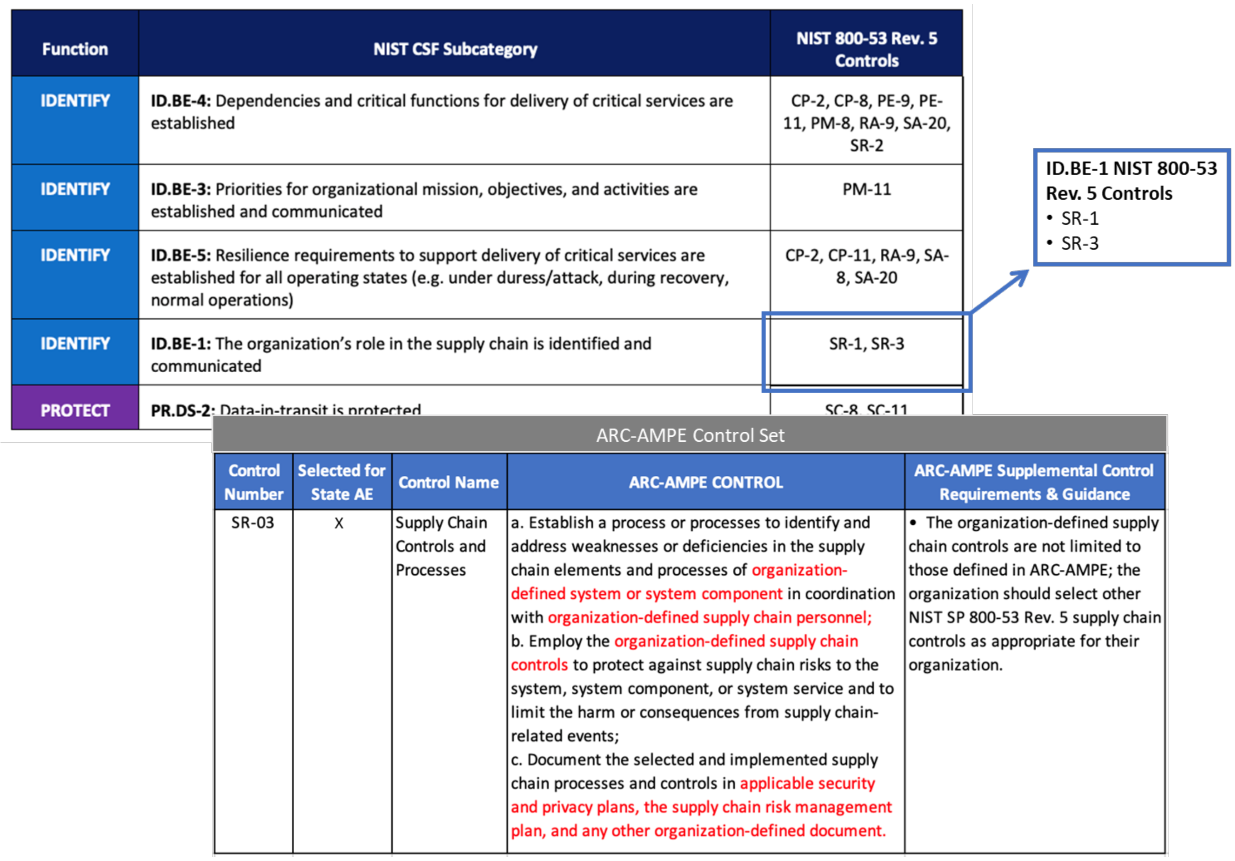
Function	NIST CSF Subcategory	NIST SP 800-53 Rev. 5 Controls
PROTECT	**PR.AC-3:** Remote access is managed	AC-1, AC-17, AC-19, AC-20, SC-15
PROTECT	**PR.AC-6:** Identities are proofed and bound to credentials and asserted in interactions	AC-16, IA-1, IA-2, IA-4, IA-5, IA-8, IA-12, PE-2, PS-3
PROTECT	**PR.AC-7:** Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	AC-14, IA-1, IA-2, IA-3, IA-5, IA-8, IA-9, IA-10, IA-11
PROTECT	**ID.AM-5:** Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	CP-2, RA-2, RA-9, SA-20, SC-6
PROTECT	**PR.DS-7:** The development and testing environment(s) are separate from the production environment	CM-2
PROTECT	**PR.AC-4:** Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24
PROTECT	**PR.AC-5:** Network integrity is protected (e.g., network segregation, network segmentation)	AC-4, AC-10, SC-7, SC-10, SC-20
PROTECT	**RS.MI-1:** Incidents are contained	IR-4
PROTECT	**RC.RP-1:** Recovery plan is executed during or after cybersecurity incident	CP-10, IR-4, IR-8
PROTECT	**DE.CM-1:** The network is monitored to detect potential cybersecurity events	AU-12, CA-7, CM-3, SC-5, SC-7, SI-4
PROTECT	**DE.CM-4:** Malicious code is detected	SC-44, SI-3, SI-4, SI-8

Function	NIST CSF Subcategory	NIST SP 800-53 Rev. 5 Controls
PROTECT	**DE.CM-8:** Vulnerability scans are performed	RA-5
PROTECT	**DE.CM-3:** Personnel activity is monitored to detect potential cybersecurity events	AC-2, AU-12, AU-13, CA-7, CM-10, CM-11
PROTECT	**DE.CM-5:** Unauthorized mobile code is detected	SC-18, SC-44, SI-4
PROTECT	**DE.CM-6:** External service provider activity is monitored to detect potential cybersecurity events	CA-7, PS-7, SA-4, SA-9, SI-4
PROTECT	**DE.CM-7:** Monitoring for unauthorized personnel, connections, devices, and software is performed	AU-12, CA-7, CM-3, CM-8, PE-6, PE-20, SI-4
PROTECT	**RC.IM-1:** Recovery plans incorporate lessons learned	CP-2, IR-4, IR-8

D.2.2 Relationship between the ACA AE CSF Profile and *ARC-AMPE Volume II*

Figure 4 shows the relationship between the ACA AE CSF Profile and *ARC-AMPE Volume II*. Using the High and Moderate Priority CSF Subcategories, CMS compared the mapped NIST SP 800-53 Rev. 5 controls with the controls in the *ARC-AMPE Volume II*. As a result, CMS considered controls mapped to a High or Moderate Priority Subcategory that were not initially included in *ARC-AMPE Volume II* (based on the NIST Moderate baseline) and determined whether those controls should be tailored into the ACA AE CSF Profile.

CMS also used mapped controls to confirm their inclusion in the *ARC-AMPE Volume II*. For instance, SR-3 requires an entity to establish and document Supply Chain plans and processes that may be time intensive and require coordination across the entity's organization and other partners. Identification and communication of the entity's role in the supply chain (ID.BE-1), however, is considered High Priority due to an ACA AE's role in operating an Exchange and making Quality Health Plans available. Therefore, a state benefits by establishing these processes and controls to minimize supply chain risks. Devoting resources to implementing SR-3 can also help address or lay the groundwork for other High Priority Subcategories, such as identifying weaknesses in protecting established critical functions and their dependencies (ID.BE-4).



Function	NIST CSF Subcategory	NIST 800-53 Rev. 5 Controls
IDENTIFY	**ID.BE-4:** Dependencies and critical functions for delivery of critical services are established	CP-2, CP-8, PE-9, PE-11, PM-8, RA-9, SA-20, SR-2
IDENTIFY	**ID.BE-3:** Priorities for organizational mission, objectives, and activities are established and communicated	PM-11
IDENTIFY	**ID.BE-5:** Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	CP-2, CP-11, RA-9, SA-8, SA-20
IDENTIFY	**ID.BE-1:** The organization's role in the supply chain is identified and communicated	SR-1, SR-3
PROTECT	**PR.DS-2:** Data-in-transit is protected	SC-8, SC-11

ID.BE-1 NIST 800-53 Rev. 5 Controls
- SR-1
- SR-3

ARC-AMPE Control Set

Control Number	Selected for State AE	Control Name	ARC-AMPE CONTROL	ARC-AMPE Supplemental Control Requirements & Guidance
SR-03	X	Supply Chain Controls and Processes	a. Establish a process or processes to identify and address weaknesses or deficiencies in the supply chain elements and processes of organization-defined system or system component in coordination with organization-defined supply chain personnel; b. Employ the organization-defined supply chain controls to protect against supply chain risks to the system, system component, or system service and to limit the harm or consequences from supply chain-related events; c. Document the selected and implemented supply chain processes and controls in applicable security and privacy plans, the supply chain risk management plan, and any other organization-defined document.	• The organization-defined supply chain controls are not limited to those defined in ARC-AMPE; the organization should select other NIST SP 800-53 Rev. 5 supply chain controls as appropriate for their organization.

Figure 4. Relationship of ACA AE CSF Profile to the *ARC-AMPE Volume II*

Organizations should consider all CSF Subcategories regardless of prioritization indicated in this Profile. Subcategory prioritization enables an entity to review the *ARC-AMPE Volume II* against prioritized Subcategories and determine if resources are adequately allocated. Evaluating the Profile and prioritized Subcategories can also help an entity determine if they are placing an emphasis on implementation of certain controls. For instance, an entity may focus their planning on Other Priority cybersecurity outcomes, such as investigating notifications from detection systems (RS.AN-1), without implementing such High Priority Subcategories as establishing critical functions and dependencies (ID.BE-4) that require detection systems. Reviewing the *ARC-AMPE Volume II* and prioritized Subcategories may help entities identify gaps in assets or processes that align with a given Subcategory. An entity can then adjust their cybersecurity risk management program and communicate priorities to stakeholders within the organization.

D.2.3 NIST Privacy Framework Profile Use Case

Using a similar methodology, CMS developed an ACA AE Privacy Framework Profile by reusing the Pillars from the ACA AE CSF Profile. This process required evaluating a Subcategory's priority against the Pillars. CMS identified the elements of the NIST Privacy Framework v1.0 Core (i.e., Functions, Categories, Subcategories) that support achieving the ACA AE Use Case Pillars. In doing so, CMS prioritized the organization's privacy obligations against enterprise business functions.

D.2.3.1 Determine Prioritization Methodology for Privacy Outcomes

Determining how a Privacy Framework Subcategory may affect a Pillar can help an entity identify the relative privacy risk against its organizational goals. Table 9 and Table 10 present the High and Moderate Subcategories,[120] respectively, for the ACA AE Privacy Framework Profile. CMS grouped the Privacy Framework v1.0 Subcategories consistent with the levels established for the CSF Profile.

Table 9. Privacy Framework High Priority Subcategories for the ACA AE Use Case

Function	NIST Privacy Framework Subcategory	NIST SP 800-53 Rev. 5 Controls
IDENTIFY-P	**ID.IM-P2**: Owners or operators (e.g., the organization or third parties such as service providers, partners, customers, and developers) and their roles with respect to the systems/products/services and components (e.g., internal or external) that process data are inventoried.	CM-8(4), CM-13
IDENTIFY-P	**ID.IM-P3:** Categories of individuals (e.g., customers, employees or prospective employees, consumers) whose data are being processed are inventoried.	CM-13
IDENTIFY-P	**ID.IM-P4:** Data actions of the systems/products/services are inventoried.	CM-13
IDENTIFY-P	**ID.IM-P5:** The purposes for the data actions are inventoried.	CM-13, PT-1, PT-2, PT-3
IDENTIFY-P	**ID.IM-P6**: Data elements within the data actions are inventoried.	CM-13, PM-5(1), PT-7
IDENTIFY-P	**ID.IM-P7:** The data processing environment is identified (e.g., geographic location, internal, cloud, third parties).	CM-8, CM-12, CM-13
IDENTIFY-P	**ID.IM-P8:** Data processing is mapped, illustrating the data actions and associated data elements for systems/products/services, including components; roles of the component owners/operators; and interactions of individuals or third parties with the systems/products/services.	CM-13
IDENTIFY-P	**ID.BE-P1:** The organization's role(s) in the data processing ecosystem are identified and communicated.	SR-1, SR-3
IDENTIFY-P	**ID.BE-P2:** Priorities for organizational mission, objectives, and activities are established and communicated.	PM-11
IDENTIFY-P	**ID.BE-P3:** Systems/products/services that support organizational priorities are identified and key requirements communicated.	RA-9
GOVERN-P	**GV.PO-P3:** Roles and responsibilities for the workforce are established with respect to privacy.	All -1 controls, CP-2, PM-2, PM-3, PM-13, PM-18, PM-19, PM-29, PS-7, PS-9

[120] *NIST Privacy Framework v. 1.0* mapping to NIST SP 800-53 Rev 5 controls is available at: "Mappings: Cybersecurity Framework and Privacy Framework to Revision 5," https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final.

Function	NIST Privacy Framework Subcategory	NIST SP 800-53 Rev. 5 Controls
GOVERN-P	**GV.PO-P4:** Privacy roles and responsibilities are coordinated and aligned with third-party stakeholders (e.g., service providers, customers, partners).	PM-18, PM-19, PM-29
GOVERN-P	**GV.PO-P5:** Legal, regulatory, and contractual requirements regarding privacy are understood and managed.	all -1 controls
GOVERN-P	**GV.PO-P6:** Governance and risk management policies, processes, and procedures address privacy risks.	PM-3, PM-7, PM-9, PM-10, PM-11, PM-18, PM-19, PM-23, PM-28, RA-1, RA-3, RA-8
GOVERN-P	**GV.AT-P1:** The workforce is informed and trained on its roles and responsibilities.	AT-2, AT-3, AT-3(3), AT-3(5), PM-13, PM-14
GOVERN-P	**GV.AT-P3:** Privacy personnel understand their roles and responsibilities.	AT-3, AT-3(3), AT-3(5), CP-3, IR-2, IR-2(3), PM-13
GOVERN-P	**GV.MT-P3:** Policies, processes, and procedures for assessing compliance with legal requirements and privacy policies are established and in place.	CA-2, CA-7, PM-14, PM-31
GOVERN-P	**GV.MT-P7:** Policies, processes, and procedures for receiving, tracking, and responding to complaints, concerns, and questions from individuals about organizational privacy practices are established and in place.	PM-20, PM-22, PM-26, SI-18
CONTROL-P	**CT.PO-P1:** Policies, processes, and procedures for authorizing data processing (e.g., organizational decisions, individual consent), revoking authorizations, and maintaining authorizations are established and in place.	PT-1, PT-2, PT-3, PT-4
CONTROL-P	**CT.PO-P2:** Policies, processes, and procedures for enabling data review, transfer, sharing or disclosure, alteration, and deletion are established and in place (e.g., to maintain data quality, manage data retention).	AC-1, AC-3(14), CM-9, MP-6, PM-22, PM-23, SI-12, SI-18
COMMUNICATE-P	**CM.AW-P5:** Data corrections or deletions can be communicated to individuals or organizations (e.g., data sources) in the data processing ecosystem.	PM-22, SI-18(5)
COMMUNICATE-P	**CM.AW-P7:** Impacted individuals and organizations are notified about a privacy breach or event.	IR-1, IR-2(3), IR-4, IR-6, IR-8
PROTECT-P	**PR.PO-P7:** Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are established, in place, and managed.	CP-1, CP-2, CP-7, CP-10, IR-1, IR-7, IR-8, IR-9
PROTECT-P	**PR.AC-P5:** Network integrity is protected (e.g., network segregation, network segmentation).	AC-4, AC-10, SC-7, SC-10, SC-20
PROTECT-P	**PR.DS-P1:** Data-at-rest are protected.	MP-2, MP-3, MP-4, MP-5, MP-6, MP-7, MP-8, SC-28
PROTECT-P	**PR.DS-P2:** Data-in-transit are protected.	SC-8, SC-11
PROTECT-P	**PR.DS-P4:** Adequate capacity to ensure availability is maintained.	AU-4, CP-2, PE-11, SC-5

Function	NIST Privacy Framework Subcategory	NIST SP 800-53 Rev. 5 Controls
PROTECT-P	**PR.DS-P5:** Protections against data leaks are implemented.	AC-4, AC-5, AC-6, AU-13, PE-19, PS-6, SC-7, SI-4
PROTECT-P	**PR.PT-P3:** Communications and control networks are protected.	AC-12, AC-17, AC-18, CP-8, SC-5, SC-7, SC-10, SC-11, SC-20, SC-21, SC-22, SC-23, SC-31, SC-37, SC-38, SC-47

Table 10. Privacy Framework Moderate Priority Subcategories for the ACA AE Use Case

Function	NIST Privacy Framework Subcategory	NIST SP 800-53 Rev. 5 Controls
IDENTIFY-P	**ID.IM-P1:** Systems/products/services that process data are inventoried.	CM-8, CM-12, CM-13, PM-5
IDENTIFY-P	**ID.RA-P1:** Contextual factors related to the systems/products/services and the data actions are identified (e.g., individuals' demographics and privacy interests or perceptions, data sensitivity and/or types, visibility of data processing to individuals and third parties).	CM-13, PM-5(1), PT-7, RA-3, RA-8
IDENTIFY-P	**ID.RA-P2:** Data analytic inputs and outputs are identified and evaluated for bias.	Not mapped
IDENTIFY-P	**ID.RA-P3:** Potential problematic data actions and associated problems are identified.	CM-13, RA-3, RA-8
IDENTIFY-P	**ID.RA-P4:** Problematic data actions, likelihoods, and impacts are used to determine and prioritize risk.	PM-28, RA-2, RA-3, RA-8
IDENTIFY-P	**ID.RA-P5:** Risk responses are identified, prioritized, and implemented.	CA-5, PM-4, PM-9, PM-28, RA-7, RA-8
IDENTIFY-P	**ID.DE-P1:** Data processing ecosystem risk management policies, processes, and procedures are identified, established, assessed, managed, and agreed to by organizational stakeholders.	PM-30, SA-9, SR-1, SR-2, SR-3, SR-4, SR-5
IDENTIFY-P	**ID.DE-P2:** Data processing ecosystem parties (e.g., service providers, customers, partners, product manufacturers, application developers) are identified, prioritized, and assessed using a privacy risk assessment process.	PM-9, RA-3, RA-8, SA-15, SR-2, SR-3, SR-5, SR-6
IDENTIFY-P	**ID.DE-P3:** Contracts with data processing ecosystem parties are used to implement appropriate measures designed to meet the objectives of an organization's privacy security and privacy requirements.	SA-4, SA-9, SR-2, SR-3, SR-5, SR-8
IDENTIFY-P	**ID.DE-P5:** Data processing ecosystem parties are routinely assessed using audits, test results, or other forms of evaluations to confirm if the party is meeting its contractual, interoperability framework, or other obligations.	AU-6, CA-2, CA-7, PS-7, SA-9, SA-11

Function	NIST Privacy Framework Subcategory	NIST SP 800-53 Rev. 5 Controls
GOVERN-P	**GV.PO-P1:** Organizational privacy values and policies (e.g., conditions on data processing such as data uses or retention periods, individuals' prerogatives with respect to data processing) are established and communicated.	all -1 controls
GOVERN-P	**GV.PO-P2:** Processes to instill organizational privacy values within system/product/service development and operations are established and in place.	PM-3, PM-23, SA-2, SA-3
GOVERN-P	**GV.RM-P1:** Risk management processes are established, managed, and agreed to by organizational stakeholders.	PM-9, PM-28
GOVERN-P	**GV.RM-P2:** Organizational risk tolerance is determined and clearly expressed.	PM-9
GOVERN-P	**GV.RM-P3:** The organization's determination of risk tolerance is informed by its role(s) in the data processing ecosystem.	PM-28
GOVERN-P	**GV.AT-P2:** Senior executives understand their roles and responsibilities.	AT-3, PM-13
GOVERN-P	**GV.AT-P4:** Third parties (e.g., service providers, customers, partners) understand their roles and responsibilities.	AT-3, PS-7, SA-9
GOVERN-P	**GV.MT-P1:** Privacy risk is re-evaluated on an ongoing basis and as key factors, including the organization's business environment (e.g., introduction of new technologies), governance (e.g., legal obligations, risk tolerance), data processing, and systems/products/services change.	CA-7, CA-7(4), CM-4, CM-13, PM-5(1), RA-3, RA-8
GOVERN-P	**GV.MT-P2:** Privacy values, policies, and training are reviewed, and any updates are communicated.	all -1 controls
GOVERN-P	**GV.MT-P4:** Policies, processes, and procedures for communicating progress on managing privacy risks are established and in place.	CA-5, PM-4, PM-27
GOVERN-P	**GV.MT-P5**: Policies, processes, and procedures are established and in place to receive, analyze, and respond to problematic data actions disclosed to the organization from internal and external sources (e.g., internal discovery, privacy researchers, professional events).	CM-4, PM-15, RA-3, RA-8, SI-19(8)
CONTROL-P	**CT.PO-P3:** Policies, processes, and procedures for enabling individuals' data processing preferences and requests are established and in place.	AC-1, AC-3(14), PT-1, PT-4, SI-18, PM-22
CONTROL-P	**CT.DM-P1:** Data elements can be accessed for review.	AC-2, AC-3, AC-3(14), CM-2, CM-3, CM-6, SI-18
CONTROL-P	**CT.DM-P2:** Data elements can be accessed for transmission or disclosure.	AC-2, AC-3, AC-4, AC-21, CM-2, CM-3, CM-6, SI-18
CONTROL-P	**CT.DM-P3:** Data elements can be accessed for alteration.	AC-2, AC-3, CM-2, CM-3, CM-6, SI-18
CONTROL-P	**CT.DM-P4:** Data elements can be accessed for deletion.	AC-2, AC-3, CM-2, CM-3, CM-6, SI-12, SI-18
CONTROL-P	**CT.DM-P5:** Data are destroyed according to policy.	MP-6, SI-12(3), SR-12

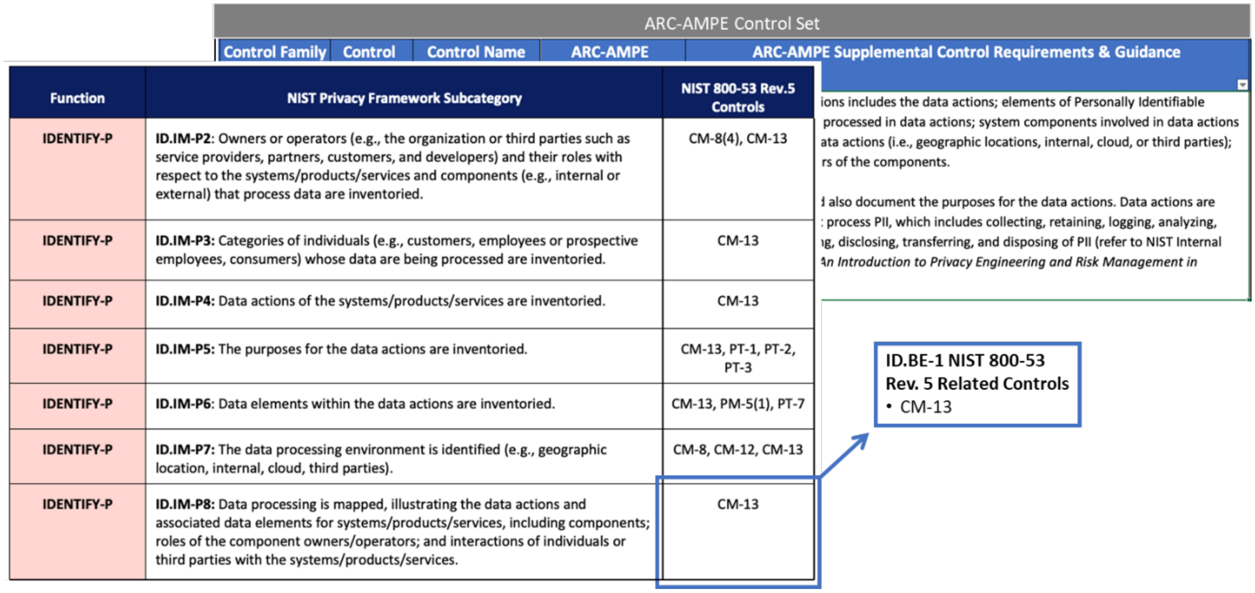
Function	NIST Privacy Framework Subcategory	NIST SP 800-53 Rev. 5 Controls
COMMUNICATE-P	**CM.PO-P1:** Transparency policies, processes, and procedures for communicating data processing purposes, practices, and associated privacy risks are established and in place.	PM-20, PM-27, PT-1, PT-2, PT-3, PT-5, PT-6, RA-8
COMMUNICATE-P	**CM.PO-P2:** Roles and responsibilities (e.g., public relations) for communicating data processing purposes, practices, and associated privacy risks are established.	PT-1
COMMUNICATE-P	**CM.AW-P1:** Mechanisms (e.g., notices, internal or public reports) for communicating data processing purposes, practices, associated privacy risks, and options for enabling individuals' data processing preferences and requests are established and in place.	AC-8, PT-5, PM-20, SC-42(4)
COMMUNICATE-P	**CM.AW-P4:** Records of data disclosures and sharing are maintained and can be accessed for review or transmission/disclosure.	PM-21
PROTECT-P	**PR.PO-P1:** A baseline configuration of information technology is created and maintained incorporating security principles (e.g., concept of least functionality).	CM-1, CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10
PROTECT-P	**PR.PO-P2:** Configuration change control processes are established and in place.	CM-3, CM-4, SA-10
PROTECT-P	**PR.PO-P3:** Backups of information are conducted, maintained, and tested.	CP-4, CP-6, CP-9
PROTECT-P	**PR.AC-P1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized individuals, processes, and devices.	IA-1, IA-2, IA-3, IA-4, IA-5, IA-7, IA-8, IA-9, IA-10, IA-11, IA-12
PROTECT-P	**PR.AC-P2:** Physical access to data and devices is managed.	PE-1, PE-2, PE-3, PE-4, PE-5, PE-6, PE-8, PE-9
PROTECT-P	**PR.AC-P3:** Remote access is managed.	AC-1, AC-17, AC-19, AC-20, SC-15
PROTECT-P	**PR.AC-P4:** Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.	AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24
PROTECT-P	**PR.AC-P6**: Individuals and devices are proofed, bound to credentials, and authenticated commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).	AC-14, AC-16, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11, IA-12, PE-2, PS-3
PROTECT-P	**PR.DS-P3:** Systems/products/services and associated data are formally managed throughout removal, transfers, and disposition.	CM-8, MP-6, PE-16, PE-20
PROTECT-P	**PR.DS-P7:** The development and testing environment(s) are separate from the production environment.	CM-2(6)
PROTECT-P	**PR.MA-P1:** Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools.	MA-1, MA-2, MA-3, MA-5, MA-6
PROTECT-P	**PR.MA-P2:** Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.	MA-4

Function	NIST Privacy Framework Subcategory	NIST SP 800-53 Rev. 5 Controls
PROTECT-P	**PR.PT-P1:** Removable media is protected, and its use restricted according to policy.	MP-1, MP-2, MP-3, MP-4, MP-5, MP-7, MP-8
PROTECT-P	**PR.PT-P2:** The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.	AC-3, CM-7
PROTECT-P	**PR.PT-P4:** Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations.	CP-7, CP-8, CP-11, CP-12, CP-13, PE-11, PL-8, SC-6

D.2.4 Relationship between the ACA AE Privacy Framework Profile and *ARC-AMPE Volume II*

As shown in the tables, most of the Subcategories prioritized as High and Moderate are from the Identify-P, Govern-P, and Protect-P Functions. These Functions' Subcategories were considered the most critical, from a privacy perspective, to support the ACA AE Use Case Pillars and identify critical functions and dependencies, establish clear governance processes, and protect an organization's assets and data.

Figure 5 shows the relationship between the ACA AE Privacy Framework Profile and *ARC-AMPE Volume II*. For example, additional resources may be necessary to develop and document a map of system data actions (CM-13); however, the ACA AE Privacy Framework Profile demonstrates inventory and mapping (ID.IM-P8) as a High Priority to inform an entity of privacy risks. Processing Personally Identifiable Information may be a key component of an ACA AE's operations and essential to achieving its guiding Pillars. If the entity notes a deficiency in how it understands data processing by its assets, the entity may devote more resources or planning toward implementing control CM-13, which is included in the *ARC-AMPE Volume II*. This action enables the entity to better address the Data Processing High Priority Subcategories.



ARC-AMPE Control Set

Control Family	Control	Control Name	ARC-AMPE	ARC-AMPE Supplemental Control Requirements & Guidance
				ions includes the data actions; elements of Personally Identifiable processed in data actions; system components involved in data actions ata actions (i.e., geographic locations, internal, cloud, or third parties); rs of the components. d also document the purposes for the data actions. Data actions are : process PII, which includes collecting, retaining, logging, analyzing, ng, disclosing, transferring, and disposing of PII (refer to NIST Internal *An Introduction to Privacy Engineering and Risk Management in*

Function	NIST Privacy Framework Subcategory	NIST 800-53 Rev.5 Controls
IDENTIFY-P	**ID.IM-P2**: Owners or operators (e.g., the organization or third parties such as service providers, partners, customers, and developers) and their roles with respect to the systems/products/services and components (e.g., internal or external) that process data are inventoried.	CM-8(4), CM-13
IDENTIFY-P	**ID.IM-P3:** Categories of individuals (e.g., customers, employees or prospective employees, consumers) whose data are being processed are inventoried.	CM-13
IDENTIFY-P	**ID.IM-P4:** Data actions of the systems/products/services are inventoried.	CM-13
IDENTIFY-P	**ID.IM-P5:** The purposes for the data actions are inventoried.	CM-13, PT-1, PT-2, PT-3
IDENTIFY-P	**ID.IM-P6**: Data elements within the data actions are inventoried.	CM-13, PM-5(1), PT-7
IDENTIFY-P	**ID.IM-P7:** The data processing environment is identified (e.g., geographic location, internal, cloud, third parties).	CM-8, CM-12, CM-13
IDENTIFY-P	**ID.IM-P8:** Data processing is mapped, illustrating the data actions and associated data elements for systems/products/services, including components; roles of the component owners/operators; and interactions of individuals or third parties with the systems/products/services.	CM-13

Figure 5. Relationship of the ACA AE Privacy Framework Profile to *ARC-AMPE Volume II*

Subcategories not categorized as High or Moderate Priority were designated as “Other Priority.” Implementers of the Profile can rely on Other Priority Subcategories to better manage their budgets and resources.

D.3 Considerations for Applying the NIST CSF and Privacy Framework

ARC-AMPE Volume II provides the minimum security and privacy controls for ACA operations. An entity’s information systems may be required to meet additional security control requirements as mandated by specific sources, whether federal, state, local, legal, or program regulations. The NIST CSF and Privacy Frameworks can help an organization align its strategic activities with its priorities. By reviewing the NIST Frameworks and Profiles, an entity can determine the need for additional controls or more stringent control parameters to achieve organization-specific strategic goals.

An entity benefits by using Profiles to assess its progress toward achieving its goal cybersecurity posture (i.e., implementing High and Moderate priority outcomes and mapped controls). The assessment should examine the current people, processes, and technologies that implement security and privacy functions, as well as the entity’s progress toward full implementation. The assessment may reveal gaps, for example, because too many resources are allocated to “Other Priority” items while High and Moderate priority items have yet to be addressed. To address any gaps, an entity should develop action plans or processes to shift focus and resources to implement the controls mapped to High and Moderate priority Subcategories.

Acronyms

Term	Definition
ABE	Agent/Broker Entity
ACA	Patient Protection and Affordable Care Act
AE	Administering Entities
AMPE	ACA, Medicaid, and Partner Entities
API	Application Programming Interface
ARC	Acceptable Risk Controls
ARPA	American Rescue Plan Act
ARS	Acceptable Risk Safeguards
ATC	Authority to Connect
BA	Business Associate
BHP	Basic Health Program
CAA	Consolidated Appropriations Act of 2021
CE	Covered Entity
CFR	Code of Federal Regulations
CHIP	Children’s Health Insurance Program
CMA	Computer Matching Agreement
CMS	Centers for Medicare & Medicaid Services
CN	Change Notification
CSF	NIST Cybersecurity Framework
CUI	Controlled Unclassified Information
DE	Direct Enrollment
DHS	Department of Homeland Security
DoD	Department of Defense
DUA	Data Use Agreement
EDE	Enhanced Direct Enrollment
EO	Executive Order
ERM	Enterprise Risk Management
FedRAMP	Federal Risk and Authorization Management Program
FFE	Federally-facilitated Exchange

Term	Definition
FIPS	Federal Information Processing Standards
FIPPs	Fair Information Practice Principles
FISMA	Federal Information Security Management Act of 2002; Federal Information Security Modernization Act of 2014
FPL	Federal Poverty Line
FTI	Federal Tax Information
GRC	Governance, Risk Management, and Compliance
HHS	Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act of 1996
HITECH	Health Information Technology for Economic and Clinical Health Act
HPH	Healthcare and Public Health
Hub	CMS Federal Data Services Hub
IEA	Information Exchange Agreement
IES	Integrated Eligibility & Enrollment System
IIHI	Individually Identifiable Health Information
IR	NIST Interagency Report
IRA	Inflation Reduction Act
IRC	Internal Revenue Code
IRS	Internal Revenue Service
IS2P	HHS Information Security and Privacy Policy
IS2P2	CMS Information Systems Security and Privacy Policy
ISA	Interconnection Security Agreement
ISCM	Information Security Continuous Monitoring
ISRA	Information System Risk Assessment
IT	Information Technology
MARS-E	Minimum Acceptable Risk Standards for Exchanges
MMIS	Medicaid Management Information System
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NEE	Non-Exchange Entity
NEE GRC	Non-Exchange Entity Governance, Risk Management, and Compliance Framework

Term	Definition
NIST	National Institute of Standards and Technology
NSA	No Surprises Act
OMB	Office of Management and Budget
ONC	Office of National Coordinator for Heath Information Technology
OpDiv	Department of Health and Human Services Operating Division
OPM	Office of Personnel Management
PHI	Protected Health Information
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
POA&M	Plan of Actions and Milestones
QHP	Qualified Health Plan
RA	Risk Acceptance Form
RMF	NIST Risk Management Framework
RSP	Recognized Security Practice
RTC	Request to Connect
SAP	Security Assessment Plan
SAR	Security Assessment Report
SAW	Security Assessment Workbook
SBE	State-based Exchange
SBE-FP	State-based Exchange on the Federal Platform
SHOP	Small Business Health Options Program
SIA	Security Impact Assessment
SP	Service Provider
SP	Special Publication
SSA	Social Security Administration
SSPP	System Security and Privacy Plan
TEFCA	Trusted Exchange Framework and the Common Agreement
U.S.C.	United States Code
VA	Department of Veterans Affairs

List of References

Centers for Medicare & Medicaid Services (CMS) Affordable Care Act (ACA) Security and Privacy Policies, Guidance, Procedures, and Templates

1. Annual Security and Privacy Attestation Procedures for State-Based ACA Administering Entity Systems, available at: https://zone.cms.gov/document/annual-security-and-privacy-attestation-procedure-aca-systems.
2. Security and Privacy Oversight and Monitoring Guide for Administering Entity (AE) Systems in Operation, available at: https://zone.cms.gov/document/security-and-privacy-oversight-and-monitoring-guide-ae-systems-operation.
3. Change Reporting Procedures for State-Based Administering Entity Systems, available at: https://zone.cms.gov/document/change-reporting-procedures-administering-entities-aca-systems.
4. Framework for Independent Assessment of Security and Privacy Controls, available at: https://zone.cms.gov/document/framework-independent-assessment-security-and-privacy-controls.
5. Decommissioning Guide for Administering Entity ACA Systems, available at: https://zone.cms.gov/document/decommissioning-and-data-retention-planning.
6. Administering Entity Security and Privacy Incident Report template, available at: https://zone.cms.gov/document/aca-administering-entity-ae-incident-response-ir.
7. Fed2NonFed Interconnection Security Agreement template, available at: https://zone.cms.gov//document/fed2nonfed-interconnection-security-agreement-isa.
8. State Plan of Action and Milestones, Template, available at: https://zone.cms.gov/document/plan-action-and-milestones-template.
9. Information Security Risk Assessment (ISRA) Template Instructions, available at: https://zone.cms.gov/document/information-security-risk-assessment-isra-procedures-administering-entities.
10. Affordable Care Act Health Insurance Administering Entity Privacy Impact Assessment (PIA) template and guide, available at: https://zone.cms.gov/document/privacy-impact-assessment-pia.
11. Information Exchange Agreement Template, available at: https://zone.cms.gov//document/information-exchange-agreement-iea.
12. Computer Matching Agreement (CMA) between CMS and State-Based Administering Entities, available at: https://zone.cms.gov/document/computer-matching-agreement.

13. CMS Security and Privacy MARS-E Timelines and Artifacts List: available at: https://zone.cms.gov/document/cms-security-and-privacy-mars-e-timelines-and-artifacts-list.

14. CMS Acceptable Risk Safeguards (ARS): https://www.cms.gov/research-statistics-data-and-systems/cms-information-technology/informationsecurity/information/acceptable-risk-safeguards-50x.

Federal Legislation, Guidance, and Regulations

1. Public Law 111–148, Patient Protection and Affordable Care Act, March 23, 2010, 124 Stat. 119, available at: https://www.congress.gov/111/plaws/publ148/PLAW-111publ148.pdf.

2. Public Law 74-271, Social Security Act, as amended, available at: http://www.ssa.gov/OP_Home/ssact/ssact.htm.

3. Public Law 93-579, The Privacy Act of 1974, September 27, 1975, 88 Stat. 1896, 5 U.S.C. §552a, as amended, available at: https://www.archives.gov/about/laws/privacy-act-1974.html.

4. Public Law 104-13, Paperwork Reduction Act of 1995, as amended, available at: http://www.fws.gov/policy/library/rgpl104-13.pdf.

5. Code of Federal Regulations (CFR), Regulation 5 CFR Part 731 – Suitability, 5CFR731. Available at: https://www.govinfo.gov/app/details/CFR-2012-title5-vol2/CFR-2012-title5-vol2-sec731-202.

6. United States Code Title 44, Chapter 33—Disposal of Records, available at: http://www.archives.gov/about/laws/disposal-of-records.html.

7. *Federal Information System Controls Audit Manual (FISCAM)*, Government Accountability Office, GAO-09-232G, February 2, 2009, available at: http://www.gao.gov/new.items/d09232g.pdf.

8. Office of Management and Budget (OMB), Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information,* January 3, 2017, available at: https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2017/m-17-12_0.pdf.

9. NIST SP 800-37 Rev. 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, December 2018, available at: https://www.nist.gov/publications/risk-management-framework-information-systems-and-organizations-system-life-cycle.

10. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev. 5, *Security and Privacy Controls for Information Systems and Organizations*, December 10, 2020, available at: https://www.nist.gov/publications/security-and-privacy-controls-information-systems-and-organizations-0.

11. NIST SP 800-53A Rev. 5, *Assessing Security and Privacy Controls in Information Systems and Organizations*, December 10, 2014, available at: https://www.nist.gov/publications/assessing-security-and-privacy-controls-federal-information-systems-and-organizations.

12. NIST SP 800-53B, *Control Baselines for Information Systems and Organizations*, October 29, 2020, available at: https://csrc.nist.gov/pubs/sp/800/53/b/final.

13. NIST SP 800-63-3, *Digital Identity Guidelines,* March 2, 2020, available at: https://csrc.nist.gov/publications/detail/sp/800-63/3/final.

14. NIST SP 800-66 Rev. 2, *Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide,* February 2024, available at: https://csrc.nist.gov/pubs/sp/800/66/r2/final.

15. NIST SP 800-145, *The NIST Definition of Cloud Computing*, September 2011, available at: https://csrc.nist.gov/publications/detail/sp/800-145/final.

16. NIST SP 800-88 Revision 1, *Guidelines for Media Sanitization*, December 2014, available at: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf.

17. *NIST Framework for Improving Critical Infrastructure Cybersecurity* v.1.1 (also known as the NIST Cybersecurity Framework), February 19, 2014, available at: https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity. (Refer to version 2.0, February 26, 2024. Available at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf.)

18. *NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management*, Version 1.0, January 16, 2020, available at: CSWP 10, NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0 | CSRC.

19. Federal Information Processing Standards (FIPS) Publication (PUB) 199, *Standards for Security Categorization of Federal Information and Information Systems,* NIST, February 2004, available at: https://csrc.nist.gov/csrc/media/publications/fips/199/final/documents/fips-pub-199-final.pdf.

20. FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, NIST, May 2006, available at: http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf.

21. Internal Revenue Service Publication 1075, *Tax Information Security Guidelines for Federal, State and Local Agencies and Entities*, can be found at: http://www.irs.gov/pub/irs-pdf/p1075.pdf.

22. *e-Government Act of 2002*. https://www.congress.gov/107/plaws/publ347/PLAW-107publ347.pdf.

23. Federal Information Security Management Act of 2002, available at: http://csrc.nist.gov/groups/SMA/fisma/index.html.

24. Health Insurance Portability and Accountability Act of 1996, available at: http://www.gpo.gov/fdsys/pkg/PLAW-104publ191/content-detail.html.

25. Privacy Act of 1974, available at: https://www.cms.gov/PrivacyActof1974/.

26. Department of Health and Human Services Final Rule on Exchange Establishment Standards and Other Related Standards under the Affordable Care Act, 45 CFR Parts 155, 156, and 157, March 12, 2012, as amended.