Beyond Compliance

Why ARC-AMPE is the New Standard for Trust in Healthcare IT

Written by:
Daniel Wright & Kenice Middleton

Special Contributions by:
Rica Vasquez

WHITEPAPER

Stewarding organizations through a dynamic global economy, we deliver **trusted** solutions that protect data, preserve resources, ensure compliance, and optimize operations.

Contents

Overview

The protection of health information is a national priority. As healthcare delivery systems modernize and cybersecurity threats become more sophisticated, the safeguarding of sensitive data—including Personally Identifiable Information (PII) and Protected Health Information (PHI)—is essential to upholding public trust and ensuring operational integrity. In response to these growing demands, the Centers for Medicare & Medicaid Services (CMS) has introduced **Acceptable Risk Controls for ACA, Medicaid, and Provider Entities (ARC-AMPE).** This new framework replaces the outdated Minimum Acceptable Risk Safeguards for Exchanges (MARS-E) standard and aligns healthcare risk and compliance operations with **National Institute of Standards and Technology Special Publication (NIST SP) 800-53 Revision 5.**

ARC-AMPE presents a paradigm shift. It emphasizes integrated privacy, continuous monitoring, and outcome-based controls tailored to the realities of modern health IT environments. With a 12-month mandate for adoption across all 50 states and some U.S. territories, ARC-AMPE is not just an ehanced security requirement—it is a strategic imperative for protecting data, maintaining Authority-to-Connect (ATC) eligibility, and enabling scalable, secure service delivery.

A holistic ARC-AMPE implementation strategy weaves together three interconnected phases: assessment, implementation, and continuous monitoring.

01

Assessment

This process begins by taking a comprehensive look at the organization's existing environment-examining system boundaries, evaluating current risk levels, and measuring how well existing practices align with ARC-AMPE requirements.

02

Implementation

From there, implementation becomes a targeted effort, rolling out customized controls, technologies, and governance structures that reflect the unique challenges and priorities uncovered during the assessment.

03

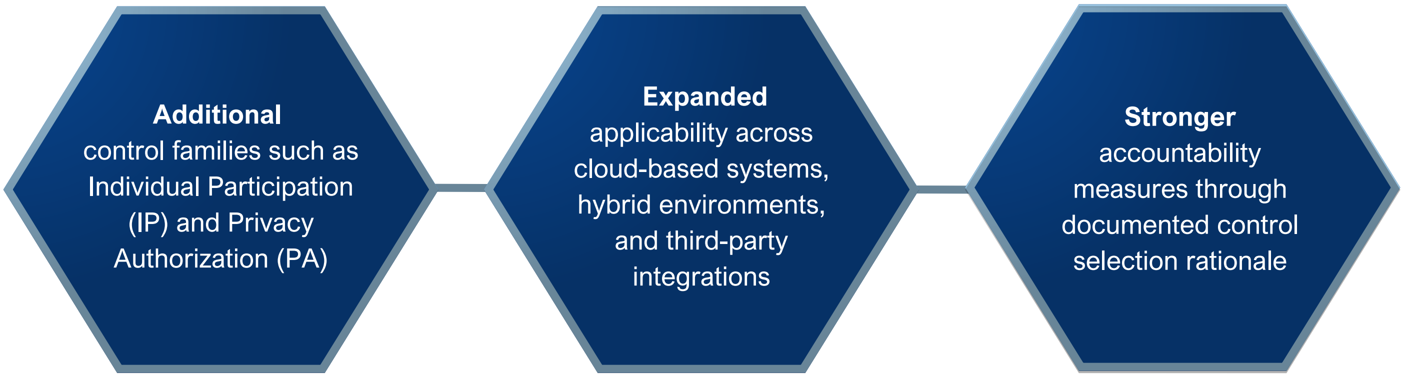
Continuous Monitoring

This isn't a one-time fix; the final phase, continuous monitoring, ensures that safeguards remain effective, responsive, and aligned with the evolving cybersecurity and regulatory landscape.

☑ **Taken together, this strategic approach enables organizations to not only to meet CMS mandates but also to build long-term security, privacy, and operational resilience.**

From MARS-E to ARC-AMPE

The legacy MARS-E framework, based on NIST SP 800-53 Rev. 4, lacks the breadth of privacy integration and specificity now required in complex, interoperable systems. ARC-AMPE, built on **NIST SP 800-53 Rev. 5,** addresses these gaps by embedding privacy controls directly into the security catalog and creating a unified language for risk management across public and private sectors. Key updates include:



Additional control families such as Individual Participation (IP) and Privacy Authorization (PA)

Expanded applicability across cloud-based systems, hybrid environments, and third-party integrations

Stronger accountability measures through documented control selection rationale

These changes reflect the federal government's commitment to advancing both **cybersecurity and data privacy** through a more integrated and proactive risk management approach.

Safeguarding What Matters Most

Healthcare data breaches have become increasingly common and costly. ARC-AMPE directly addresses these threats by enabling organizations to identify and mitigate privacy and security risks across digital ecosystems. It strengthens the protection of sensitive health data throughout its lifecycle while ensuring alignment with CMS ATC requirements for connectivity to federal systems.

Moreover, ARC-AMPE supports continuous compliance and audit readiness. With PII and PHI as high-value targets, ARC-AMPE’s alignment with Rev. 5 is particularly significant. Privacy is no longer an adjacent consideration—it is embedded within the security framework, ensuring that access control, consent, transparency, and individual rights are addressed as part of a cohesive defense strategy.

Understanding the Landscape

Effective ARC-AMPE implementation begins with comprehensive assessment. Organizations should start with a boundary analysis to map system interfaces and understand data flows. This is followed by a risk assessment incorporating interviews, document reviews, and technical scans to identify vulnerabilities and process inefficiencies. A thorough gap analysis then compares current practices with ARC-AMPE requirements to highlight deficiencies and prioritize remediation. These foundational activities build a strong baseline for an effective ARC-AMPE integration. As part of this process, organizations should prioritize their efforts by first identifying controls that are entirely new under ARC-AMPE, as these typically require the greatest level of effort and planning to implement. Following that, attention should shift to controls that have changed in scope or parameters compared to their MARS-E 2.2 counterparts, necessitating updates to existing processes and documentation. Finally, controls that remain unchanged from MARS-E 2.2 should be re-evaluated in context, confirming that previous implementations are still appropriate and effective under the new framework. This tiered approach to control analysis ensures that implementation efforts are focused where they are needed most, promoting efficiency and enabling smarter resource allocation.

Turning Insight into Action: Tailoring ARC-AMPE

Following assessment, implementation must be deliberate and adaptable. Organizations should create tailored implementation plans that align with the most pressing risks and resource constraints. This includes assigning clear responsibilities, establishing measurable milestones, and applying modern security tools that align with organizational capacity.

Technologies and frameworks should be selected for their effectiveness and efficiency, ensuring optimal results without unnecessary complexity. Staff should be trained on new controls and procedures, while change management efforts help embed these practices into day-to-day operations. A successful rollout depends on both technological precision and organizational alignment.

Keeping the Pulse: Monitoring, Adapting, and Improving

ARC-AMPE requires a commitment to ongoing evaluation and enhancement. Maintaining Plan of Action and Milestones (POA&Ms) are essential to tracking progress and ensuring accountability. Periodic reassessments should be conducted to respond to new threats or system changes, while all control selections and updates must be documented for audit readiness. Leveraging automated tools for monitoring, reporting, and risk visualization enhances transparency and responsiveness. This commitment to continuous improvement helps organizations stay resilient in the face of shifting regulatory and threat landscapes.

Small but Mighty: The Power of Small Business in ARC-AMPE Success

Small businesses play a critical role in successful ARC-AMPE implementation. Their agility enables rapid customization for diverse environments, and their cost-effective services are often ideal for conducting assessments, providing technical support, and facilitating training.

Small firms often take on program management roles, overseeing timelines, stakeholder coordination, and oversight responsibilities. They also drive innovation through the use of modern Governance, Risk, and Compliance (GRC) platforms and cloud-native technologies. These partnerships expand the reach of internal teams and can provide the specialized expertise needed to meet ARC-AMPE objectives efficiently and sustainably.

Conclusion

ARC-AMPE represents a critical modernization effort in federal and state healthcare compliance. By transitioning from MARS-E to this NIST Rev. 5-aligned framework, organizations can elevate their data security posture, meet evolving CMS mandates, and safeguard patient trust. A successful ARC-AMPE journey requires assessment, customization, strategic implementation, and continuous evaluation. When supported by skilled partners—including small businesses—organizations are well-positioned to meet today's challenges and tomorrow's opportunities with resilience and accountability.

About TWW

The Wright Way Enterprises (TWW) is certified as an SBA 8(a) and HUBZone small business, stewarding organizations in addressing the dynamic needs of an ever-changing global economy. Founded in 2020, TWW’s comprehensive capabilities fortify federal and private infrastructure. The impact-driven consultancy specializes in program management, auditing, cyber risk management, and compliance. TWW's vision is to be globally trusted advisors in delivering robust solutions that protect data, preserve vital resources, ensure compliance, and optimize operations for excellence. TWW’s counsel includes business and IT consulting, change management, capacity assessments, strategic planning, financial analysis, process improvement, audit, and compliance. For more information, visit www.twwenterprises.com.

Website: www.twwenterprises.com

Email: contact@twwenterprises.com

LinkedIn: twwenterprises

Instagram: @twwenterprises