SmartSuite

Framework / Risk Management / NIST Special Publications

CMS MARS-E v2.0

MARS-E v2.0 establishes baseline cybersecurity controls for health insurance exchanges handling federal data, ensuring data protection and regulatory compliance.

What it is

U.S. CMS MARS-E v2.0 (Minimum Acceptable Risk Standards for Exchanges) is a cybersecurity and compliance framework that establishes baseline security requirements for health insurance exchanges handling federal data. It supports organizations in safeguarding sensitive data, managing risks, and meeting federal regulatory obligations related to the operation of health insurance marketplaces.

Developed by the Centers for Medicare & Medicaid Services (CMS), MARS-E v2.0 is used by state and federal health insurance exchanges, contractors, and related entities. The framework covers areas such as access control, incident response, risk management, data protection, and privacy governance, aligning with federal standards like NIST SP 800-53 to ensure consistency in security practices.

At a glance

PUBLISHER Centers for Medicare & Medicaid Services (CMS)	TYPE Control Framework	VERSION v2.0
EFFECTIVE September 23, 2015	DOMAIN Risk Management	FAMILY NIST Special Publications
REGION United States	INDUSTRY Insurance	ADOPTION MODEL Regulatory Compliance
IMPLEMENTATION COMPLEXITY High		

Source: https://www.cms.gov/cciio/resources/regulations-and-guidance/downloads/2-mars-e-v2-0-minimum-acceptable-risk-standards-for-exchanges-11102015.pdf

Why it matters

- **Strengthen cybersecurity governance** Establishes clear requirements and oversight for managing risks and protecting health data within exchange environments.
- **Enable stronger regulatory compliance** Aligns security practices with federal mandates, supporting organizations in meeting CMS and related regulatory requirements.
- **Enhance audit readiness** Standardizes documentation and reporting, making it easier for organizations to demonstrate compliance during internal and external audits.
- **Improve data protection practices** Implements controls that safeguard personally identifiable and protected health information against unauthorized access and misuse.

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports CMS MARS-E v2.0

MARS-E Control Library

Structure CMS MARS-E security and privacy controls with mapped responsibilities and implementation tasks.

System Security and Privacy Governance

Track policies, procedures, and system safeguards protecting healthcare exchange data.

Risk Assessments and Authorization Management

Manage risk assessments, authorization activities, and ongoing system security reviews.

Vulnerability and Incident Management

Track vulnerability findings, remediation activities, and incident response workflows affecting exchange systems.

Vendor and System Integration Oversight

Monitor security requirements and compliance evidence for partners supporting healthcare exchange operations.

CMS Security Assessment Readiness Reporting

Provide dashboards showing control coverage, remediation progress, and readiness for CMS security assessments.

Common framework mappings

CIS Controls v8.1 | HIPAA (NIST SP 800-66 Rev. 2) | HITRUST CSF v11.5 | ISO 27001:2022 | NIST CSF 2.0 | NIST 800-53 Rev.5 | SOC 2

Official resources

CMS MARS-E v2.0 Framework

Provides baseline security requirements for health insurance exchanges handling federal data.

cms.gov/cciio/resources/regulations-and-guidance/downloads/2-mars-e-v2-0-minimum-acceptable-risk-standards-for-exchanges-11102015.pdf

Frequently asked questions

What is MARS-E v2.0 used for?

MARS-E v2.0 is used to establish minimum security and privacy requirements for health insurance exchanges that process, store, or transmit federal data. Its primary goal is to protect sensitive health information and ensure compliance with federal cybersecurity mandates in the operation of health insurance marketplaces.

Is compliance with MARS-E v2.0 mandatory?

Yes, MARS-E v2.0 compliance is mandatory for state and federal health insurance exchanges and any entities, contractors, or business associates that handle federal health data on their behalf. Adherence is required to meet regulatory obligations mandated by the Centers for Medicare & Medicaid Services (CMS).

What is the scope of MARS-E v2.0?

The scope of MARS-E v2.0 covers all information systems, processes, and entities involved in the collection, storage, processing, or transmission of federal health data within health insurance exchanges. This includes internal systems, third-party vendors, and any infrastructure supporting exchange operations.

What are the key control families and artifacts in MARS-E v2.0?

MARS-E v2.0 aligns with NIST SP 800-53 and contains control families addressing access control, risk assessment, incident response, security training, system integrity, and privacy governance. Key artifacts include system security plans (SSPs), risk assessments, policies and procedures, incident response plans, and compliance documentation.

 Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How do organizations implement MARS-E v2.0?

Organizations implement MARS-E v2.0 by mapping required security controls to operational processes, developing policies to address each control, and conducting regular risk assessments. Implementation involves technical, procedural, and administrative safeguards along with ongoing monitoring and documentation of compliance activities.

How does MARS-E v2.0 relate to other cybersecurity frameworks?

MARS-E v2.0 is closely aligned with federal standards like NIST SP 800-53, sharing similar control structures, terminology, and security objectives. It is tailored specifically for health insurance exchanges and provides additional privacy and risk protection requirements relevant to the federal health data environment.

What are the ongoing compliance requirements for MARS-E v2.0?

Maintaining MARS-E v2.0 compliance requires periodic internal and external risk assessments, continuous monitoring of security controls, timely remediation of security gaps, and up-to-date documentation. Organizations must also prepare for independent audits and provide evidence of control effectiveness to regulatory bodies.

How would SmartSuite support MARS-E v2.0?

SmartSuite supports MARS-E v2.0 compliance by providing centralized control management, automated risk and issue tracking, and streamlined evidence collection. The platform enables organizations to manage compliance workflows, prepare for audits, and generate real-time reports on MARS-E controls, ensuring comprehensive oversight and audit readiness.

License included / downloadable: Yes CMS MARS-E v2.0 is publicly available for download from the CMS website. License included with platform

Full framework page and mappings: smartsuite.com/frameworks/us-cms-mars-e-v20-minimum-acceptable-risk-standards-for-exchanges

 © 2026 SmartSuite Inc. All rights reserved.