Understand MARS-E security requirements and learn how health insurance exchanges impact your organization.

Background

With the enactment of the Patient Protection and Affordable Care Act (ACA) of 2010, which created the federal and state health insurance exchanges (HIXs or marketplaces), one of the new compliance requirements for security is known as Minimum Acceptable Risk Standards for Exchanges (MARS-E).

What is MARS-E?

Section 1561 of ACA requires the U.S. Department of Health and Human Services (HHS) to develop interoperable and secure standards and protocols to facilitate the electronic enrollment of individuals in HIXs. Unfortunately, there is no integrated, comprehensive approach to security and privacy that respects federal requirements under other state and federal legislation or regulations. To facilitate compliance with the myriad of security requirements for HIX and enrollment systems, the Centers for Medicare and Medicaid Services (CMS) developed MARS-E with a two-fold purpose — to provide:

- Security guidance for state and federal HIXs concerning Personally Identifiable Information (PII), Protected Health Information (PHI) or Federal Tax Information (FTI) of U.S. citizens

- Guidance for state and federal HIXs and their contractors regarding the minimum-level security controls that must be implemented to protect information and information systems that CMS oversees

MARS-E requires state and federal HIX enrollment systems to address certain federal legislation and regulations, including:

- Federal Information Security Management Act (FISMA) of 2002: Controls the development, documentation and implementation of programs providing security for information and information systems
- Health Insurance Portability and Accountability Act (HIPAA): Established national standards for electronic healthcare transactions and national identifiers for providers, health insurance plans and employers, setting privacy and security standards for handling health information
- Health Information Technology for Economic and Clinical Health (HITECH) Act: Offers incentives to healthcare providers for demonstrating meaningful use of electronic health records (EHRs), with penalties for non-compliance after 2014
- HHS final rule on Exchange Establishment Standards and Other Related Standards (under the ACA, 45 Code of Federal Regulations (CFR) Parts 155, 156 and 157, March 12, 2012): Establishes privacy and security controls required for processing exchange applicant information
- Internal Revenue Code (IRC), 26 U.S.C. Section 6103: Establishes criteria for handling FTI

Security control areas for MARS-E

Protecting and ensuring the confidentiality, integrity and availability of HIX and enrollment systems is the joint responsibility of HIXs and CMS. Since HIXs and CMS must share data and integrate IT systems for the implementation and operation of HIXs, MARS-E defines a minimum set of standards for 17 specific "security control families" for acceptable security risk that HIXs must address. They are:

1. Access control
2. Awareness and training
3. Audit and accountability
4. Security assessment and authorization
5. Configuration management.
6. Contingency planning
7. Identification and authentication
8. Incident response
9. Maintenance
10. Media protection
11. Physical and environment protection
12. Planning
13. Personnel security
14. Risk assessment
15. System and services acquisition
16. Systems and communication protection
17. Systems and information integrity

Also, the MARS-E document contains standards for two other areas:

- Program management (PM): Complements the security controls in the above 17 families by focusing on the organization-wide requirements essential for managing information security programs.
- FTI safeguards: Lists additional controls required by IRS Publication 1075.

MARS-E is also supported by the Catalog of Minimum Acceptable Risk Controls for Exchanges – Exchange Reference Architecture Supplement which provides technical and operational details for each of the security controls. The catalog provides methodology for determining the availability of security controls for each of the 17 security control families.

Will MARS-E impact my organization?

Due to the complexity of meeting all of the security requirements of MARS-E, you are probably concerned about whether MARS-E applies to you or not. Many organizations, including America's Health Insurance Plans (AHIP) and the Association for Community Affiliated Plans (ACAP), relayed their concerns to CMS about their members' ability to meet MARS-E security standards. As a result, CMS issued two letters, dated August 28, 2013, and September 4, 2013, to issuers like you concerning MARS-E applicability[2].

> A "captive" agent/broker who does not maintain an electronic record system for maintenance of data related to the FFM is not required to establish and implement a MARS-E compliant electronic record system in order to comply, and neither does the issuer to which the agent/broker is "captive."

In those letters, CMS stated that as long as you (including your captive agents/brokers) are not directly providing application assistance on your own systems (but can do so on the federally facilitated marketplace, known as the FFM) or are only providing enrollment functions, then MARS-E is not applicable to you. Additionally, when accessing your systems and the FFM, the workplace and computers must be compliant with the guidance offered in the September 4, 2013, letter.

Actions you can take

You will need to continue ensuring your systems comply with HIPAA, while following any other applicable security regulations (such as the Payment Card Industry Data Security Standard). In order to accomplish this, you must ensure the following:

- Your staff members, including captive agents or brokers, are not accessing, creating, collecting, maintaining or storing any PII on non-compliant systems
- Protocols are established (such as policies and procedures, training) to ensure your staff does not step out of security boundaries when providing application assistance and qualified health plan enrollment — including not recording PII, PHI or FTI outside of the systems designed for such information
- The development and deployment of workplaces and IT systems (including computers, laptops, smartphones and other electronic devices) that meet CMS security standards to reduce the risk of access to or release of PII, PHI or FTI

Failure to follow these protocols could cause your systems to become subject to MARS-E requirements and the penalties resulting from non-compliance.

Dell has worked with many of the nation's leading issuers — using proven practices and expert guidance — and can assist your organization in navigating the pitfalls of security compliance. Let us help you meet today's requirements and tomorrow's challenges.

For more information about any of our service offerings, please visit Dell.com/services or contact your Dell representative.

[1] MARS-E is a CMS-published suite of documents (version 1.0 released August 1, 2012) that defines the security standards required pursuant to 45 CFR 155.260 and 45 CFR 155.270, for any HIX, individual or entity gaining access to information submitted to a HIX or through a HIX using a direct, system-to-system connection to the CMS federal Data Services Hub.

[2] Centers for Medicare and Medicaid Services, letter, Frequently Asked Questions regarding Qualified Health Plan (QHP) Issuers and Captive Agents, issued August 28, 2013.

Scan or click this code to learn how Dell Services can help your organization.

November 2013 | D343 - HIX Compliance - Understanding MARS-E brochure.indd | Rev. 1.0