DEPARTMENT OF HEALTH AND HUMAN SERVICES
Centers for Medicare & Medicaid Services
7500 Security Boulevard, Mail Stop S2-26-12
Baltimore, MD 21244-1850

CMCS Informational Bulletin

DATE: September 23, 2015

FROM: Tim Hill, Deputy Director
Center for Medicaid and CHIP Services

SUBJECT: **Minimum Acceptable Risk Standards for Exchanges (MARS-E) 2.0**

This Informational Bulletin is intended to introduce the publication of the MARS-E 2.0 suite of documents which replaces the MARS-E 1.0 document suite, published in August 2012.

The information in the MARS-E document suite addresses the mandates of the Patient Protection and Affordable Care Act of 2010 and the Department of Health and Human Services (HHS) Affordable Care Act Regulations (45 CFR §§155.260 and 155.280), and now applies to all Affordable Care Act Administering Entities (AEs) to include Exchanges or Marketplaces, whether Federal, state, Medicaid Agencies, Children's Health Insurance Program (CHIP) agencies, state agencies administering the Basic Health Program (BHP), as well as all contractors and subcontractors.

The purpose of MARS-E is to provide security information aimed to protect and ensure the confidentiality, integrity and availability of Personally Identifiable Information (PII), Protected Health Information (PHI) or Federal Tax Information (FTI) of enrollees of Administering Entities. MARS-E 2.0 is comprised of security updates that respond to the National Institute of Standards and Technology (NIST) updates and the evolving technology and threat space such as mobile and cloud computing, insider threat, applications security, advanced persistent threat, supply chain risks, trustworthiness, assurance and resilience of systems.

Applicability to Medicaid/CHIP

The Patient Protection and Affordable Care Act of 2010 (hereafter referred to simply as the "Affordable Care Act"), provides as described in Section 1411(g) of the Affordable Care Act, the confidentiality of applicant information is a primary consideration and applicant information may only be used for the purposes of, and to the extent necessary in, ensuring the efficient operation of the Exchange. HHS has recognized the importance of incorporating security and privacy standards into the Health Insurance Exchange (HIE) program. 45 CFR §155.260 serves as the cornerstone for protecting the privacy and security of PII; it permits the collection, creation, use, and disclosure of PII only for the performance of the functions of Exchanges (per 45 CFR §155.200).

Section 155.260 (a)(3) requires Exchanges to establish and implement security and privacy standards consistent with the eight Fair Information Practice Principles (FIPP): (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. Section 155.260 (e) requires agreements between Exchanges and agencies administering Medicaid, CHIP, or the BHP for the exchange of eligibility information to meet any applicable requirements under §155.260. Medicaid and CHIP downstream entities must comply with any applicable requirements under §155.260.

Drivers for MARS-E 2.0 Update

Since publication of MARS-E 1.0 in 2012, several Federal government regulations and documents have been revised, including the following:

- NIST SP 800-53 Rev4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013.
- NIST SP 800-53A Rev4, Assessing Security and Privacy Controls in Federal Information Systems and Organizations, December 2014.
- Updates to HHS ACA-related regulations since 2012. 45 CFR § 155.260 Privacy and Security of Personally Identifiable Information was amended in March, 2014 with clarifications on data sharing, and the privacy and security standards to which an Exchange binds non-Exchange entities.
- CMS published the Acceptable Risk Safeguards (ARS) 2.0, September 2013. MARS-E 2.0 is consistent with ARS 2.0 as interpreted for the ACA Administering Entity environment.
- The IRS revised requirements for safeguarding Federal Taxpayer Information (FTI), 2014.

MARS-E 2.0 Documentation Suite

MARS-E 2.0 is a suite of four documents:

- Volume I: Harmonized Security and Privacy Framework. This is a high-level introduction of Affordable Care Act Security and Privacy policy and standards as a framework for compliance governance.

- Volume II: Minimum Acceptable Risk Standards for Exchanges. This volume introduces the concept of a Catalog of Controls; one catalog for security and another for privacy. This volume also has two appendices: 1) Security Controls Selection Table, showing MARS-E V1.0, NIST 800-53 Rev4 Moderate Baseline, ARS 2.0, and MARS-E V2.0 control set; and 2) Mapping of 45 CFR §155.260 to MARS-E Security and Privacy Controls.

- Volume III: Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges. This volume contains the security and privacy control tables. It also contains the *IRS Requirements for Safeguarding FTI* in Appendix A.

- Volume IV: ACA Administering Entity System Security Plan. This is a consolidated volume containing System Security Plan (SSP) Instructions and fill-in the blanks

template for SSP Content.

MARS-E Update Impact to Medicaid/CHIP

A new catalog of privacy controls has been added to MARS-E 2.0. All Administering Entities will be required to submit documentation of privacy control implementation details as part of their SSP. This now includes Medicaid/CHIP Agencies, as Administering Entities, who must now submit an Affordable Care Act Health Insurance Administering Entity Privacy Impact Assessment (PIA) to CMS. Previously, only state-based Marketplaces had to submit a PIA to CMS.

Introduction of Privacy Controls

The following privacy control families are new to MARS-E 2.0:

- Authority and Purpose: Ensures that organizations: (i) identify the legal bases that authorize a particular PII collection or activity that impacts privacy; and (ii) specify in their notices the purpose(s) for which PII is collected.

- Accountability, Audit, and Risk Management: Enhances public confidence through effective controls for governance, monitoring, risk management, and assessment to demonstrate that organizations are complying with applicable privacy protection requirements and minimizing overall privacy risk.

- Data Quality and Integrity: Enhances public confidence that any PII collected and maintained by organizations is accurate, relevant, timely, and complete for the purpose for which it is to be used, as specified in public notices.

- Data Minimization and Retention: Helps organizations implement the data minimization and retention requirements to collect, use, and retain only PII that is relevant and necessary for the purpose for which it was originally collected. Organizations retain PII for only as long as necessary to fulfill the purpose(s) specified in public notices and in accordance with a National Archives and Records Administration (NARA)-approved record retention schedule.

- Individual Participation and Redress: Addresses the need to make individuals active participants in the decision-making process regarding the collection and use of their PII. By providing individuals with access to PII and the ability to have their PII corrected or amended, as appropriate, the controls in this family enhance public confidence in organizational decisions made based on the PII.

- Security: Supplements the security controls in Appendix F to ensure that technical, physical, and administrative safeguards are in place to protect PII collected or maintained by organizations against loss, unauthorized access, or disclosure, and to ensure that planning and responses to privacy incidents comply with OMB policies and guidance. The controls in this family are implemented in coordination with information security personnel and in accordance with the existing NIST Risk Management Framework.

- Transparency: Ensures that organizations provide public notice of their information practices and the privacy impact of their programs and activities.

- Use Limitation: Ensures that organizations only use PII either as specified in their public notices, in a manner compatible with those specified purposes, or as otherwise permitted by law. Implementation of the controls in this family will ensure that the scope of PII use is limited accordingly.

For those with access to the Collaborative Application Lifecycle Tool (CALT), a copy of the MARS-E 2.0 close-to-final draft has been made available for states at: https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/

For questions or more information about MARS-E 2.0 and its application to Medicaid and CHIP agencies in states not operating their own state-based marketplace, please contact Marty Rice, Director Division of State Systems (DSS) at Martin.Rice1@cms.hhs.gov.