Centers for Medicare & Medicaid Services

MARS-E Document Suite, Version 2.0

Volume II: Minimum Acceptable Risk Standards for Exchanges

Version 2.0

November 10, 2015

Foreword

In accordance with the agency's Information Security program, the Centers for Medicare & Medicaid Services (CMS) has assembled a document suite of guidance, requirements, and templates known as the *Minimum Acceptable Risk Standards for Exchanges (MARS-E)*, Version 2.0. The guidance in the MARS-E document suite addresses the mandates of the Patient Protection and Affordable Care Act of 2010 (hereafter simply the "Affordable Care Act" or "ACA"), and applies to all ACA Administering Entities. "Administering Entity" means Exchanges or Marketplaces, whether federal or state, state Medicaid agencies, Children's Health Insurance Program (CHIP) agencies, or state agencies administering the Basic Health Program.

Version 2.0 of the MARS-E document suite consists of four companion documents:

- *Volume I: Harmonized Security and Privacy Framework*, Version 2.0
- *Volume II: Minimum Acceptable Risk Standards for Exchanges*, Version 2.0
- *Volume III: Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges*, Version 2.0
- *Volume IV: ACA Administering Entity System Security Plan*, Version 2.0

This suite of documents defines a risk-based Security and Privacy Framework for use in the design and implementation of Exchange information technology (IT) systems for which CMS has oversight responsibility.

Any changes to *Volume II: Minimum Acceptable Risk Standards for Exchanges* or to the MARS-E document suite must be approved by the CMS Chief Information Officer, CMS Senior Agency Official for Privacy, and the CMS Chief Information Security Officer.

Document History

Several factors necessitated update of MARS-E Version 1.0 (published August 1, 2012):

(a) To add new security controls contained in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, that are useful for managing ACA systems in today's threat environment;

(b) To add a Catalog of Privacy Controls to facilitate the management of privacy of ACA systems and leverage the new families for privacy controls introduced in NIST SP 800-53 Rev 4;

(c) To communicate implementation standards for key security and privacy controls that are consistent with the updated specifications of privacy and security requirements contained Department of Health and Human Services ACA Regulations (45 CFR §§155.260 and 155.280); and

(d) To communicate revised Internal Revenue Service (IRS) requirements [(IRS Publication 1075, *Tax Information Security Guidelines for Federal, State and Local Agencies* for safeguarding Federal Tax Information (FTI)].

Based on CMS's deeper understanding of the operating environment of state-provided ACA Administering Entity systems, and with the experience using the procedures and templates contained in MARS-E Version 1.0, the agency made the following adjustments in this release of MARS-E:

- Not all of the systems process FTI. In Version 1.0 of MARS-E, FTI protection requirements were specified in individual security controls. In Version 2.0, however, individual controls do not contain FTI protection implementation details. Instead, applicable FTI protection requirements are presented separately in Appendix A of *Volume IV: ACA Administering Entity System Security Plan*.
- MARS-E Version 1.0 used three documents within the MARS-E suite to provide instructions for preparing the System Security Plan (SSP): (1) ACA System Security Plan Procedures, (2) ACA System Security Plan Template, and (3) ACA System Security Plan Workbook. CMS has consolidated all instructions for preparing the System Security Plan in Volume IV, which also contains the Catalog of Minimum Acceptable Risk Security and Privacy Controls. This enables the SSP author to find everything needed to complete the SSP in a single document.

Finally, Version 2.0 of this document adds several new features to facilitate easier use of the appendices and completion of the implementation requirements:

- Implementation Standards have been added to key security controls with linkages to specific CMS implementation guidance documents that reside in the CMS ACA security implementation repository on CMS's Collaborative Application Life-cycle Tool (CALT).
- Appendix A contains a Security Controls Selection Table that shows the reader how the security controls in MARS-E Version 2.0 differ from those of MARS-E Version 1.0, CMS Acceptable Risk Safeguards (ARS) 2.0, and the NIST 800-53 Rev 4 (Moderate Baseline).
- Appendix B presents a crosswalk between the specification of privacy and security requirements in 45 CFR §155.260 and the security controls contained in the MARS-E *Volume III: Catalog of Minimum Acceptable Risk Security and Privacy Controls*, Version 2.0.

Record of Changes

Version Number	Date	Author/Owner	Description of Change	CR #
1.0	August 1, 2012	CMS	Version 1.0 for publication	N/A
2.0	November 10, 2015	CMS	Version 2.0 for publication	N/A

CR: Change Request

Table of Contents

List of Tables

1. Introduction

The Patient Protection and Affordable Care Act of 2010 (hereafter referred to simply as the "Affordable Care Act" or "ACA") provides a mechanism whereby each state may develop its own health insurance Exchange. State Exchanges serve as organized marketplaces that allows consumers and small businesses to quickly compare available plan options based on price and quality, as well as benefits and services. Consumers seeking healthcare coverage can go to the health insurance Exchanges to obtain comprehensive information on coverage options currently available and make informed health insurance choices. By pooling consumers, reducing transaction costs, and increasing transparency, Exchanges create more efficient and competitive health insurance markets for individuals and small employers.

As described in Section 1411(g) of the Affordable Care Act, the confidentiality of applicant information is a primary ACA implementation consideration. In the Department's Final Rule on the implementation of ACA Exchanges, released on March 12, 2012, and amended in 2014, 45 CFR §155.260 provides conditions for the creation, collection, use, and disclosure of Personally Identifiable Information (PII) for the purpose of determining eligibility for enrollment in a qualified health plan.

Section 155.260 (a)(3) of the HHS Final Rule on ACA Exchanges requires each Exchange to establish and implement privacy and security standards consistent with the principles stated in §155.260 of the Rule. Section 155.260 (e) of the HHS Final Rule on ACA Exchanges requires the same of agencies administering Medicaid, Children's Health Insurance Program (CHIP), or the Basic Health Plan Program (BHP) for the exchange of eligibility information (hereafter simply "Administering Entities" or "AE").

The Department and the Centers for Medicare & Medicaid Services (CMS) are responsible for providing guidance and oversight for the Exchanges and state information technology (IT) systems that facilitate common electronic enrollment. This responsibility includes defining business, information, and technical guidance that will create a common baseline and standards for these IT system implementation activities.

As part of CMS's oversight responsibility, CMS has developed implementation standards and procedures for a number of critical security controls. References to these documents can be found within the discussion of the individual security and privacy controls. Other related documents include those developed for the CMS Information Security program that comply with federal mandates and CMS requirements for the handling and processing of CMS's information and information systems.[1]

1.1 Purpose and Scope

All Administering Entity employees, contractors, subcontractors, and their respective facilities supporting such IT systems shall observe the controls defined in *Volume III: Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges*. The purpose of this volume of the MARS-E document suite is to provide detailed background on the content of these

[1] The CMS IS web site (http://www.cms.gov/InformationSecurity/) provides a list of CMS policy documents in the Information Security and Privacy Library that apply across the IS program.

security and privacy controls and the agreed-upon direction for how the controls must be used. This document also provides master lists of acronyms and a glossary of terms for the MARS-E document suite. The Master List of References in this document acknowledges the referenced policies, guidance, procedures, and templates that should be useful to the reader.

CMS does not intend to impose a single solution on individual states through these security and privacy standards; CMS will actively seek solutions and approaches that will work effectively for small and large states. The intent is not to focus on any particular technology, but rather to provide guidance on the necessary security and privacy considerations and requirements to secure the Administering Entity systems and data to ensure public trust.

The guidance provided in the security and privacy control catalog reflects industry and government best practices to support a viable approach for both the federal government and the states.

1.2 Audience

This document is intended for use by and available to all ACA Administering Entities and their business partners, security officers, other federal agencies, and supporting contractors. This volume[2] provides guidance to Administering Entities and their contractors regarding the minimum-level security controls and privacy controls that must be implemented to protect information and information systems for which CMS has oversight responsibility.

1.3 Document Organization

This document is organized as follows:

Section		Purpose
Section 2:	Security Guidance	Provides a high-level explanation of security guidance presented in the *Minimum Acceptable Risk Security Standards for Exchanges.*
Section 3:	Privacy Guidance	Provides a high-level explanation of privacy guidance presented in the *Minimum Acceptable Risk Privacy Standards for Exchanges.*
Section 4:	Minimum Security and Privacy Controls for Exchanges Structure	Provides a high-level explanation of the Minimum Security and Privacy Controls for Exchanges structure, including Minimum Security and Privacy Controls Family Numbering and Description, Control Requirements, and Assessment Procedures.
Appendix A:	Security Controls Selection Table	Provides a correlation of the individual controls in each Security Control family to MARS-E V 1.0, NIST SP 800-53 Rev4 (Moderate Baseline), CMS ARS V 2.0, the MARS-E V 2.0, and two controls that were introduced by CMS to address risk in the ACA environment:, SC-ACA-1 and SC-ACA-2.
Appendix B:	Crosswalk to 45 CFR §155.260	Provides a mapping of 45 CFR §155.260 to MARS-E Version 2.0 Security Controls.

[2] https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/

Section	Purpose
Master List of Acronyms for MARS-E Document Suite	Defines the acronyms used in MARS-E V 2.0 document suite.
Master Glossary for MARS-E Document Suite	Defines the unique terms used in the MARS-E V2.0 document suite,
Master List of References in MARS-E Document Suite	Lists all the sources used in preparing the MARS-E V2.0 document suite.

2. Security Guidance

The security controls identified in *Volume III: Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges* focus on AE IT systems. The controls assume that the applicable IT system has the security categorization of "Moderate" and processes or stores PII. As the title indicates, the controls specified here are designed to establish a security posture that provides for minimum acceptable risk. An Administering Entity system owner may, at its discretion, strengthen control implementation beyond the defined MARS-E requirement to provide for additional protections. In some cases, the system owner may also implement cascading controls on parent systems or in parent system environments (such as those provided for physical security) so that a subordinate system may enjoy the protections offered by the parent system. This approach is referred to as "inheritance" and is broadly recognized and accepted throughout the federal government.

Based on this security strategy, CMS developed the *Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges* from those delineated in NIST SP 800-53 Rev 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* for Moderate systems. In collaboration with ACA program owners and state representatives during the analysis of HHS ACA Regulations, CMS subsequently modified these controls to reflect the environment in which ACA systems operate. Appendix A provides a Security Control Selection Table that demonstrates how MARS-E Version 2.0 controls differ from those described in MARS-E Version 1.0 and the NIST 800-53 Rev 4 Moderate Baseline set.

Not all of the systems process FTI. In Version 1.0 of MARS-E, FTI protection requirements were specified in individual security controls. In Version 2.0, however, individual controls do not contain FTI protection implementation details. Instead, applicable FTI protection requirements are presented separately in Appendix A in *Volume IV: ACA Administering Entity System Security Plan*.

The ACA Law and HHS ACA Regulations form the basis of Administering Entity IT system security requirements. Appendix B presents a crosswalk between the specification of privacy and security requirements in 45 CFR §155.260 and the high-level security controls contained in the *Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges*.

Implementation Standards have been added to key security controls with linkages to specific CMS implementation guidance documents that reside in the CMS ACA security implementation guidance repository, the CMS Collaborative Application Life-cycle Tool (CALT).[3]

[3] https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/

3. Privacy Guidance

Building appropriate privacy protections into the design of the Marketplaces is crucial to gaining the necessary public trust to make them successful. Privacy, with respect to PII, is a core value that can be obtained only with appropriate legislation, policies, procedures, and associated controls to ensure compliance with requirements. Protecting the privacy of individuals and their PII that is collected, used, maintained, shared, and disposed of by programs and information systems is a fundamental responsibility of federal and state organizations. Privacy also involves each individual's right to decide when and whether to share personal information, how much information to share, and the particular circumstances under which that information can be shared. In today's digital world, effective privacy for individuals depends on the safeguards employed within the information systems that are processing, storing, and transmitting PII and the environments in which those systems operate. Privacy is more than security, however, and includes, for example, the principles of transparency, notice, and choice.

Volume III: Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges provides a structured set of controls for protecting privacy. It is a roadmap for organizations to use in identifying and implementing privacy controls concerning the entire life cycle of PII, whether in paper or electronic form. The controls focus on information privacy as a value distinct from, but highly interrelated with, information security. Privacy controls are the administrative, technical, and physical safeguards employed within organizations to protect and ensure the proper handling of PII. Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze—and mitigate when necessary—the privacy risk.

The privacy controls are based on the Fair Information Practice Principles (FIPP) embodied in the Privacy Act of 1974, Section 208 of the E-Government Act of 2002, and Office of Management and Budget (OMB) policies. The FIPPs are designed to build public trust in the privacy practices of organizations and to help organizations avoid tangible costs and intangible damages from privacy incidents.

The requirements in 45 CFR §155.260 are the cornerstone for privacy and security of PII. It articulates HHS' commitment to incorporating the FIPPs into the framework of the Health Insurance Marketplaces program. 45 CFR §155.260(a)(3) identifies the eight privacy principles that form the basis upon which all Marketplaces are required to establish and implement security and privacy standards to safeguard the privacy of PII:

- **Individual Access:** Individuals should be provided with a simple and timely means to access and obtain their personal information in a readable form and format.
- **Correction:** Individuals should be provided with a timely means to dispute the accuracy or integrity of their individually identifiable information, and to have erroneous information corrected or have a dispute documented if their requests are denied.
- **Openness and Transparency:** The policies, procedures, and technologies that directly affect individuals and/or their individually identifiable information should be open and transparent.

- **Individual Choice:** Individuals should be provided a reasonable opportunity and capability to make informed decisions about the collection, use, and disclosure of their individually identifiable information.
- **Collection, Use, and Disclosure Limitation:** Individually identifiable information should be collected, used, and/or disclosed only to the extent necessary to accomplish a specified purpose(s) and never to discriminate.
- **Data Integrity:** Persons and entities should take reasonable steps to ensure that individually identifiable information is complete, accurate, and up to date to the extent necessary for the person's or entity's intended purposes and has not been altered or destroyed in an unauthorized manner.
- **Safeguards:** Individually identifiable information should be protected with reasonable administrative, technical, and physical safeguards to ensure its confidentiality, integrity, and availability and to prevent unauthorized or inappropriate access, use, or disclosure.
- **Accountability:** These principles should be implemented, and adherence assured, through appropriate monitoring and other means, and methods should be in place to report and mitigate non-adherence and breaches.

PII should only be used by or disclosed to those authorized to receive or view it. The Privacy Act, ACA and its implementing regulations, and state law, as applicable, also provide specific requirements regarding the implementation of these standards.

4. Minimum Acceptable Risk Security and Privacy Controls for Exchanges Structure

The structure of the *Minimum Acceptable Risk Security and Privacy Controls for Exchanges* employs NIST SP 800-53 Rev 4, *Security and Privacy Controls for Federal Information Systems and Organizations* family numbering, descriptions and control requirements; and NIST SP 800-53A Rev 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations* provides the assessment procedures. The following subsections present a description of the Family Numbering, Controls Structure, and Assessment Procedures. For the most part, these subsections comprise an abbreviated discussion of content found in the two NIST documents.

4.1 Minimum Acceptable Risk Security and Privacy Controls for Exchanges Family Numbering and Description

The *Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges* presents the comprehensive body of ACA security and privacy controls. These controls are subsequently divided into specific, closely related security groupings called "families" that are represented by a two-character identifier or "Family ID." This "Family ID" directly corresponds to those specified in the NIST security and privacy control framework. Each family contains security and privacy controls related to the security and privacy functionality of the family. Twenty-six of the NIST SP 800-53 Rev 4 control families were selected for the *Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges*. Table 1 and Table 2 summarize the control families and specify the two-character identifier associated with each family.

Table 1. Family Descriptions for Minimum Security Controls for Exchanges

Family (and Identifier)	Description
Access Control (AC)	The standards listed in this section focus on how the Exchange shall limit IT system access to authorized users and devices, as well as processes acting on behalf of authorized users or devices, and also describes the authorized transactions and functions that those users and devices are permitted to execute.
Awareness and Training (AT)	The standards listed in this section focus on how the Exchange shall: (i) ensure that managers and users of Exchange IT systems are made aware of the security risks associated with their activities and of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures related to the security of IT systems; and (ii) ensure that Exchange personnel are adequately trained to carry out their assigned IS-related duties and responsibilities.

Family (and Identifier)	Description
Audit and Accountability (AU)	The standards listed in this section focus on how the Exchange shall: (i) create, protect, and retain IT system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate IT system activity; and (ii) ensure that the actions of individual IT system users can be uniquely traced to those users so they can be held accountable for their actions.
Security Assessment and Authorization (CA)	The standards listed in this section focus on how the Exchange shall: (i) periodically assess the security controls in Exchange IT systems to determine if the controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in Exchange IT systems; (iii) authorize the operation of Exchange IT systems and any associated IT system connections; and (iv) monitor IT system security controls on an ongoing basis to ensure the continued effectiveness of the controls.
Configuration Management (CM)	The standards listed in this section focus on how the Exchange shall: (i) establish and maintain baseline configurations and inventories of Exchange IT systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for IT technology products employed in Exchange IT systems.
Contingency Planning (CP)	The standards listed in this section focus on how the Exchange shall establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for Exchange IT systems to ensure the availability of critical information resources and continuity of operations in emergency situations.
Identification and Authentication (IA)	The standards listed in this section focus on how the Exchange shall identify IT system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to Exchange IT systems.
Incident Response (IR)	The standards listed in this section focus on how the Exchange shall: (i) establish an operational incident-handling capability for Exchange IT systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) track, document, and report incidents to appropriate Exchange officials and/or authorities.
Maintenance (MA)	The standards listed in this section focus on how the Exchange shall: (i) perform periodic and timely maintenance on organizational information systems; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.
Media Protection (MP)	The standards listed in this section focus on how the Exchange shall: (i) protect IT system media, both paper and digital; (ii) limit access to information on IT system media to authorized users; and (iii) sanitize or destroy IT system media before disposal or release for reuse.

Family (and Identifier)	Description
Physical and Environmental Protection (PE)	The standards listed in this section focus on how the Exchange shall: (i) limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; (iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems.
Planning (PL)	The standards listed in this section focus on how the Exchange shall develop, document, periodically update, and implement security plans for Exchange IT systems that describe the security controls in place or planned for the IT systems and the rules of behavior for individuals accessing the IT systems.
Personnel Security (PS)	The standards listed in this section focus on how the Exchange shall: (i) ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions; (ii) ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with organizational security policies and procedures.
Risk Assessment (RA)	The standards listed in this section focus on how the Exchange shall periodically assess the risk to Exchange operations (including mission, functions, image, or reputation), Exchange assets, and individuals, resulting from the operation of Exchange IT systems and the associated processing, storage, or transmission of Exchange information.
System and Services Acquisition (SA)	The standards listed in this section focus on how the Exchange shall: (i) allocate sufficient resources to adequately protect Exchange IT systems; (ii) employ system development life cycle processes that incorporate IS considerations; (iii) employ software usage and installation restrictions; and (iv) ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization.
System and Communications Protection (SC)	The standards listed in this section focus on how the Exchange shall: (i) monitor, control, and protect Exchange communications (i.e., information transmitted or received by Exchange IT systems) at the external boundaries and key internal boundaries of the IT systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective IS within Exchange IT systems.
System and Information Integrity (SI)	The standards listed in this section focus on how the Exchange shall: (i) identify, report, and correct information and IT system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within Exchange IT systems; and (iii) monitor IT system security alerts and advisories, and take appropriate actions in response.

Family (and Identifier)	Description
Program Management (PM)	The standards listed in this section complement the security controls in the foregoing 17 security control families by focusing on the organization-wide information security requirements that are essential for managing information security programs.

Table 2. Family Descriptions for Minimum Privacy Controls for Exchanges

Family (and Identifier)	Description
Authority and Purpose (AP)	This set of controls 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 (AR)	This set of controls 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 (DI)	This set of controls 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 (DM)	These set of controls 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 state and/or federal record retention schedules, i.e., for Federally-facilitated Marketplaces (FFM) a National Archives and Records Administration (NARA)-approved record retention schedule.
Individual Participation and Redress (IP)	This family 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 (SE)	This family supplements the security controls to ensure that technical, physical, and administrative safeguards are in place to PII collected or maintained by organizations against loss, unauthorized access, or disclosure, and to ensure that planning and responses to privacy incidents comply with state requirements and/or OMB policies and guidance.
Transparency (TR)	This family ensures that organizations provide public notice of their information practices and the privacy impact of their programs and activities.
Use Limitation (UL)	This family 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.

4.2 Control Structure

The control structure consists of the following sections: Baseline Control and Implementation Standards, Enhancement Control, Guidance, Related Control Requirements, and Assessment Procedure. The following subsections provide a brief description of the structure of each section of the controls.

4.2.1 Baseline Control

Each control is assigned a control number that corresponds with recommended security and privacy practices as prescribed in NIST SP 800-53 Rev4.

Enhancement controls reflect additional safeguards to the original NIST 800-53 baseline controls that are needed in response to the evolving threat environment or to achieve a heightened level of protection as deemed necessary by CMS. An enhancement to a baseline control is denoted by an enhancement number, placed in parenthesis, following the Control Number.

The control specification is the concise statement specifying the capability needed.

4.2.1.1 Implementation Standard

When an implementation standard is indicated, it is associated with the Baseline control. Some implementation standards may contain specific recommended definitions or event values (such as “90 days”) as the compliance standard for a given control. Other implementation standards are based on specific types of data, such as PII.

4.2.2 Guidance

For the sake of clarity, some baseline controls may include a guidance section to provide additional information on the intent of the control. In some cases, that guidance will include specific CMS preferences or recommendations, or may refer to other CMS or NIST publications.

4.2.3 Related Control Requirements

Relationships between security controls and privacy controls are common. They can provide important security and privacy insights. By identifying inconsistencies between related security and privacy control implementation descriptions, state security and privacy personnel may also identify real gaps that exist in the implementation of critical security and privacy functionality. Therefore, states should carefully examine related control implementation descriptions to ensure consistency in the documentation of security controls, as well as the actual implementation of all related security features.

4.2.4 Assessment Procedures

The Assessment Procedures subsection, which consists of Assessment Objectives and Assessment Methods and Objects, provides a set of procedural steps for the Exchange to determine whether the security and privacy controls for the IT system are effective (i.e., implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security and privacy requirements of the system) during the assessment process. The Assessment Procedures, largely based on NIST SP 800-53A Rev 4, *Assessing Security and*

Privacy Controls in Federal Information Systems and Organizations, consists of one or more assessment objectives with defined assessment methods.

4.2.4.1 Assessment Objectives

Each assessment objective determination statement relates to the individual requirements as specified in either the baseline control, the enhancement control, or the implementation standards. The objective of the assessment is to address all requirements and implementation standards stated in the control description. By making certain that all of the elements in the control description are part of the assessment objective, the AE can ensure traceability of assessment results back to the fundamental control requirements. This confirms that all aspects of the security and privacy controls are assessed and any weaknesses or deficiencies in the control identified to take remediation actions.

4.2.4.2 Assessment Methods and Objects

The Assessment Methods and Objects define the nature of the assessor's actions and the associated activity (i.e., Examine, Interview, and Test). The assessment object identifies the specific item assessed, including specifications, mechanisms, activities, and individuals. If the assessment team determines that a security control is not adequately implemented, these inconsistencies will be documented as findings. These assessment findings subsequently help the Exchange determine the overall effectiveness of the control implementation.

Appendix A. Security Controls Selection Table

The following tables (Tables 3–20) correlate the individual controls in each Security Control family to MARS-E Version 1.0, National Institute of Standards and Technology Special Publication 800-53 Rev4 (Moderate Baseline), Centers for Medicare & Medicaid Services (CMS) Information Security Acceptable Risk Safeguards (ARS) Version 2.0, the MARS-E Version 2.0, and two controls introduced by CMS to address risk in the Affordable Care Act (ACA) environment:, SC-ACA-1 and SC-ACA-2.

Table 3. AC Family Controls Selection

Control No.	Control Name	MARS-E V 1.0	800-53 Rev4 MODERATE BASELINE	CMS ARS V 2.0	MARS-E V 2.0
AC-1	Access Control Policy and Procedures	AC-1	AC-1	AC-1	AC-1
AC-2	Account Management	AC-2 (2) (3) (4)	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4) (7)	AC-2 (1) (2) (3) (4) (7)
AC-3	Access Enforcement	AC-3	AC-3	AC-3 (3)	AC-3 (9)
AC-4	Information Flow Enforcement	AC-4	AC-4	AC-4	AC-4
AC-5	Separation of Duties	AC-5	AC-5	AC-5	AC-5
AC-6	Least Privilege	AC-6 (2)	AC-6 (1) (2) (5) (9) (10)	AC-6 (1) (2) (5) (9) (10)	AC-6 (1) (2) (5) (9) (10)
AC-7	Unsuccessful Logon Attempts	AC-7	AC-7	AC-7	AC-7
AC-8	System Use Notification	AC-8	AC-8	AC-8	AC-8
AC-9	Previous Logon (Access) Notification		Not Selected		
AC-10	Concurrent Session Control	AC-10	Not Selected	AC-10	AC-10
AC-11	Session Lock	AC-11	AC-11 (1)	AC-11 (1)	AC-11 (1)
AC-12	Session Termination		AC-12	AC-12	AC-12
AC-13	Withdrawn		---	---	
AC-14	Permitted Actions without Identification or Authentication	AC-14 (1)	AC-14 *(1) withdrawn	AC-14(1)	AC-14
AC-15	Withdrawn		---	---	
AC-16	Security Attributes		Not Selected	AC-16	
AC-17	Remote Access	AC-17 (1) (3)	AC-17 (1) (2) (3) (4)	AC-17 (1) (2) (3) (4)	AC-17 (1) (2) (3) (4)
AC-18	Wireless Access	AC-18 (1)	AC-18 (1)	AC-18 (1)	AC-18 (1)
AC-19	Access Control for Mobile Devices	AC-19	AC-19 (5)	AC-19 (5)	AC-19 (5)
AC-20	Use of External Information Systems	AC-20	AC-20 (1) (2)	AC-20 (1) (2)	AC-20 (1) (2)
AC-21	Information Sharing		AC-21	AC-21	AC-21
AC-22	Publicly Accessible Content		AC-22	AC-22	AC-22
AC-23	Data Mining Protection		Not Selected		
AC-24	Access Control Decisions		Not Selected		
AC-25	Reference Monitor		Not Selected		

Table 4. AT Family Controls Selection

Control No.	Control Name	MARS-E V 1.0	800-53 Rev 4 MODERATE BASELINE	CMS ARS V 2.0	MARS-E V 2.0
AT-1	Security Awareness and Training Policy and Procedures	AT-1	AT-1	AT-1	AT-1
AT-2	Security Awareness Training	AT-2	AT-2 (2)	AT-2 (2)	AT-2 (2)
AT-3	Role-Based Security Training	AT-3	AT-3	AT-3	AT-3
AT-4	Security Training Records	AT-4	AT-4	AT-4	AT-4
AT-5	**Withdrawn**		---		

Table 5. AU Family Controls Selection

Control No.	Control Name	MARS-E V 1.0	800-53 Rev 4 MODERATE BASELINE	CMS ARS V 2.0	MARS-E V 2.0
AU-1	Audit and Accountability Policy and Procedures	AU-1	AU-1	AU-1	AU-1
AU-2	Audit Events	AU-2 (4)	AU-2 (3)	AU-2 (3)	AU-2 (3)
AU-3	Content of Audit Records	AU-3 (1)	AU-3 (1)	AU-3 (1)	AU-3 (1)
AU-4	Audit Storage Capacity	AU-4	AU-4	AU-4	AU-4
AU-5	Response to Audit Processing Failures	AU-5	AU-5	AU-5	AU-5 (1)
AU-6	Audit Review, Analysis, and Reporting	AU-6 (1)	AU-6 (1) (3)	AU-6 (1) (3)	AU-6 (1) (3)
AU-7	Audit Reduction and Report Generation	AU-7 (1)	AU-7 (1)	AU-7 (1)	AU-7 (1)
AU-8	Time Stamps	AU-8 (1)	AU-8 (1)	AU-8 (1)	AU-8 (1)
AU-9	Protection of Audit Information	AU-9	AU-9 (4)	AU-9 (2) (4)	AU-9 (4)
AU-10	Non-repudiation	AU-10	Not Selected	AU-10	AU-10
AU-11	Audit Record Retention	AU-11	AU-11	AU-11	AU-11
AU-12	Audit Generation	AU-12 (1)	AU-12	AU-12 (1)	AU-12 (1)

Control No.	Control Name	MARS-E V 1.0	800-53 Rev 4 MODERATE BASELINE	CMS ARS V 2.0	MARS-E V 2.0
AU-13	Monitoring for Information Disclosure		Not Selected		
AU-14	Session Audit		Not Selected		
AU-15	Alternate Audit Capability		Not Selected		
AU-16	Cross-Organizational Auditing		Not Selected		AU-16

Table 6. CA Family Controls Selection

Control No.	Control Name	MARS-E V 1.0	800-53 Rev 4 MODERATE BASELINE	CMS ARS V 2.0	MARS-E V 2.0
CA-1	Security Assessment and Authorization Policies and Procedures	CA-1	CA-1	CA-1	CA-1
CA-2	Security Assessments	CA-2 (1)	CA-2 (1)	CA-2 (1)	CA-2 (1)
CA-3	System Interconnections	CA-3	CA-3 (5)	CA-3 (5)	CA-3 (5)
CA-4	**Withdrawn**		---		
CA-5	Plan of Action and Milestones	CA-5 (1)	CA-5	CA-5 (1)	CA-5 (1)
CA-6	Security Authorization	CA-6	CA-6	CA-6	CA-6
CA-7	Continuous Monitoring	CA-7 (1) (2)	CA-7 (1)	CA-7 (1)	CA-7 (1)
CA-8	Penetration Testing		Not Selected		
CA-9	Internal System Connections		CA-9	CA-9	CA-9

Table 7. CM Family Controls Selection

Control No.	Control Name	MARS-E V 1.0	800-53 Rev 4 MODERATE BASELINE	CMS ARS V 2.0	MARS-E V 2.0
CM-1	Configuration Management Policy and Procedures	CM-1	CM-1	CM-1	CM-1
CM-2	Baseline Configuration	CM-2 (1) (3) (4)	CM-2 (1) (3) (7)	CM-2 (1) (3) (7)	CM-2 (1) (3)
CM-3	Configuration Change Control	CM-3 (2)	CM-3 (2)	CM-3 (2)	CM-3 (2)
CM-4	Security Impact Analysis	CM-4 (1) (2)	CM-4	CM-4 (1) (2)	CM-4 (1) (2)
CM-5	Access Restrictions for Change	CM-5	CM-5	CM-5 (1) (5)	CM-5 (1) (5)
CM-6	Configuration Settings	CM-6 (3)	CM-6	CM-6 (1)	CM-6 (1)
CM-7	Least Functionality	CM-7 (1)	CM-7 (1) (2) (4)	CM-7 (1) (2) (4)	CM-7 (1) (2) (4)
CM-8	Information System Component Inventory	CM-8 (1)	CM-8 (1) (3) (5)	CM-8 (1) (3) (5)	CM-8 (1) (3) (5)
CM-9	Configuration Management Plan	CM-9	CM-9	CM-9	CM-9
CM-10	Software Usage Restrictions		CM-10	CM-10	CM-10 (1)
CM-11	User-Installed Software		CM-11	CM-11	CM-11

Table 8. CP Family Controls Selection

Control No.	Control Name	MARS-E V 1.0	800-53 Rev 4 MODERATE BASELINE	CMS ARS V 2.0	MARS-E V 2.0
CP-1	Contingency Planning Policy and Procedures	CP-1	CP-1	CP-1	CP-1
CP-2	Contingency Plan	CP-2 (1) (2)	CP-2 (1) (3) (8)	CP-2 (1) (2) (3) (8)	CP-2 (1) (2) (3) (8)
CP-3	Contingency Training	CP-3	CP-3	CP-3	CP-3
CP-4	Contingency Plan Testing	CP-4 (1)	CP-4 (1)	CP-4 (1)	CP-4 (1)
CP-5	**Withdrawn**		---		
CP-6	Alternate Storage Site	CP-6 (1) (3)	CP-6 (1) (3)	CP-6 (1) (3)	CP-6 (1) (3)
CP-7	Alternate Processing Site	CP-7 (1) (2) (3) (5)	CP-7 (1) (2) (3)	CP-7 (1) (2) (3)	CP-7 (1) (2) (3)

Control No.	Control Name	MARS-E V 1.0	800-53 Rev 4 MODERATE BASELINE	CMS ARS V 2.0	MARS-E V 2.0
CP-8	Telecommunications Services	CP-8 (1) (2)	CP-8 (1) (2)	CP-8 (1) (2)	CP-8 (1) (2)
CP-9	Information System Backup	CP-9 (1)	CP-9 (1)	CP-9 (1) (3)	CP-9 (1)
CP-10	Information System Recovery and Reconstitution	CP-10 (2) (3)	CP-10 (2)	CP-10 (2)	CP-10 (2)
CP-11	Alternate Communications Protocols		Not Selected		
CP-12	Safe Mode		Not Selected		
CP-13	Alternative Security Mechanisms		Not Selected		

Table 9. IA Family Controls Selection

Control No.	Control Name	MARS-E V 1.0	800-53 Rev 4 MODERATE BASELINE	CMS ARS V 2.0	MARS-E V 2.0
IA-1	Identification and Authentication Policy and Procedures	IA-1	IA-1	IA-1	IA-1
IA-2	Identification and Authentication (Organizational Users)	IA-2 (1) (2) (3) (8)	IA-2 (1) (2) (3) (8) (11) (12)	IA-2 (1) (2) (3) (8) (11) (12)	IA-2 (1) (2) (3) (8) (11)
IA-3	Device Identification and Authentication	IA-3	IA-3	IA-3	IA-3
IA-4	Identifier Management	IA-4	IA-4	IA-4 (4)	IA-4
IA-5	Authenticator Management	IA-5 (1) (2) (3)	IA-5 (1) (2) (3) (11)	IA-5 (1) (2) (3) (6) (7) (11)	IA-5 (1) (2) (3) (7) (11)
IA-6	Authenticator Feedback	IA-6	IA-6	IA-6	IA-6
IA-7	Cryptographic Module Authentication	IA-7	IA-7	IA-7	IA-7
IA-8	Identification and Authentication (Non-Organizational Users)	IA-8	IA-8 (1) (2) (3) (4)	IA-8 (1) (2) (3) (4)	IA-8

Control No.	Control Name	MARS-E V 1.0	800-53 Rev 4 MODERATE BASELINE	CMS ARS V 2.0	MARS-E V 2.0
IA-9	Service Identification and Authentication		Not Selected		
IA-10	Adaptive Identification and Authentication		Not Selected		
IA-11	Re-authentication		Not Selected		

Table 10. IR Family Controls Selection

Control No.	Control Name	MARS-E V 1.0	800-53 Rev 4 MODERATE BASELINE	CMS ARS V 2.0	MARS-E V 2.0
IR-1	Incident Response Policy and Procedures	IR-1	IR-1	IR-1	IR-1
IR-2	Incident Response Training	IR-2	IR-2	IR-2	IR-2
IR-3	Incident Response Testing	IR-3	IR-3 (2)	IR-3 (2)	IR-3 (2)
IR-4	Incident Handling	IR-4 (1)	IR-4 (1)	IR-4 (1)	IR-4 (1)
IR-5	Incident Monitoring	IR-5	IR-5	IR-5	IR-5
IR-6	Incident Reporting	IR-6 (1)	IR-6 (1)	IR-6 (1)	IR-6 (1)
IR-7	Incident Response Assistance	IR-7 (1)	IR-7 (1)	IR-7 (1) (2)	IR-7 (1)
IR-8	Incident Response Plan	IR-8	IR-8	IR-8	IR-8
IR-9	Information Spillage Response		Not Selected		IR-9
IR-10	Integrated Information Security Analysis Team		Not Selected		

Table 11. MA Family Controls Selection

Control No.	Control Name	MARS-E V 1.0	800-53 Rev 4 MODERATE BASELINE	CMS ARS V 2.0	MARS-E V 2.0
MA-1	System Maintenance Policy and Procedures	MA-1	MA-1	MA-1	MA-1
MA-2	Controlled Maintenance	MA-2 (1)	MA-2	MA-2	MA-2
MA-3	Maintenance Tools	MA-3 (1) (2)	MA-3 (1) (2)	MA-3 (1) (2) (3)	MA-3 (1) (2) (3)
MA-4	Nonlocal Maintenance	MA-4 (1) (2) (3)	MA-4 (2)	MA-4 (1) (2) (3)	MA-4 (1) (2) (3)
MA-5	Maintenance Personnel	MA-5	MA-5	MA-5	MA-5
MA-6	Timely Maintenance	MA-6	MA-6	MA-6	MA-6

Table 12. MP Family Controls Selection

Control No.	Control Name	MARS-E V 1.0	800-53 Rev 4 MODERATE BASELINE	CMS ARS V 2.0	MARS-E V 2.0
MP-1	Media Protection Policy and Procedures	MP-1	MP-1	MP-1	MP-1
MP-2	Media Access	MP-2 (1)	MP-2	MP-2	MP-2
MP-3	Media Marking	MP-3	MP-3	MP-3	MP-3
MP-4	Media Storage	MP-4	MP-4	MP-4	MP-4
MP-5	Media Transport	MP-5 (2) (4)	MP-5 (4)	MP-5 (4)	MP-5 (4)
MP-6	Media Sanitization	MP-6 (1) (2) (5) (6)	MP-6	MP-6 (1) (2)	MP-6 (1) (2)
MP-7	Media Use		MP-7 (1)	MP-7 (1)	MP-7 (1)
MP-8	Media Downgrading		Not Selected		
MP-CMS-1	Media-Related Records	MP-CMS-1		MP-CMS-1	MP-CMS-1

Table 13. PE Family Controls Selection

Control No.	Control Name	MARS-E V 1.0	800-53 Rev 4 MODERATE BASELINE	CMS ARS V 2.0	MARS-E V 2.0
PE-1	Physical and Environmental Protection Policy and Procedures	PE-1	PE-1	PE-1	PE-1
PE-2	Physical Access Authorizations	PE-2	PE-2	PE-2	PE-2 (1)
PE-3	Physical Access Control	PE-3	PE-3	PE-3	PE-3
PE-4	Access Control for Transmission Medium	PE-4	PE-4	PE-4	PE-4
PE-5	Access Control for Output Devices	PE-5	PE-5	PE-5	PE-5
PE-6	Monitoring Physical Access	PE-6 (1)	PE-6 (1)	PE-6 (1)	PE-6 (1)
PE-7	**Withdrawn**	PE-7 (1)	---	---	
PE-8	Visitor Access Records	PE-8	PE-8	PE-8	PE-8
PE-9	Power Equipment and Cabling	PE-9	PE-9	PE-9	PE-9
PE-10	Emergency Shutoff	PE-10	PE-10	PE-10	PE-10
PE-11	Emergency Power	PE-11	PE-11	PE-11	PE-11
PE-12	Emergency Lighting	PE-12	PE-12	PE-12	PE-12
PE-13	Fire Protection	PE-13 (1) (2) (3)	PE-13 (3)	PE-13 (1) (2) (3)	PE-13 (1) (2) (3)
PE-14	Temperature and Humidity Controls	PE-14	PE-14	PE-14	PE-14
PE-15	Water Damage Protection	PE-15	PE-15	PE-15	PE-15
PE-16	Delivery and Removal	PE-16	PE-16	PE-16	PE-16
PE-17	Alternate Work Site	PE-17	PE-17	PE-17	PE-17
PE-18	Location of Information System Components	PE-18	Not Selected	PE-18	PE-18
PE-19	Information Leakage		Not Selected		
PE-20	Asset Monitoring and Tracking		Not Selected		

Table 14. PL Family Controls Selection

Control No.	Control Name	MARS-E V 1.0	800-53 Rev 4 MODERATE BASELINE	CMS ARS V 2.0	MARS-E V 2.0
PL-1	Security Planning Policy and Procedures	PL-1	PL-1	PL-1	PL-1
PL-2	System Security Plan	PL-2	PL-2 (3)	PL-2 (3)	PL-2 (3)
PL-3	**Withdrawn**		---		
PL-4	Rules of Behavior	PL-4	PL-4 (1)	PL-4 (1)	PL-4 (1)
PL-5	**Withdrawn**	PL-5	---	--	
PL-6	**Withdrawn**	PL-6	---	--	
PL-7	Security Concept of Operations		Not Selected		
PL-8	Information Security Architecture		PL-8	PL-8	PL-8
PL-9	Central Management		Not Selected		

Table 15. PS Family Controls Selection

Control No.	Control Name	MARS-E V 1.0	800-53 Rev 4 MODERATE BASELINE	CMS ARS V 2.0	MARS-E V 2.0
PS-1	Personnel Security Policy and Procedures	PS-1	PS-1	PS-1	PS-1
PS-2	Position Risk Designation	PS-2	PS-2	PS-2	PS-2
PS-3	Personnel Screening	PS-3	PS-3	PS-3	PS-3
PS-4	Personnel Termination	PS-4	PS-4	PS-4	PS-4
PS-5	Personnel Transfer	PS-5	PS-5	PS-5	PS-5
PS-6	Access Agreements	PS-6	PS-6	PS-6	PS-6
PS-7	Third-Party Personnel Security	PS-7	PS-7	PS-7	PS-7
PS-8	Personnel Sanctions	PS-8	PS-8	PS-8	PS-8

Table 16. RA Family Controls Selection

Control No.	Control Name	MARS-EV 1.0	800-53 Rev 4 MODERATE BASELINE	CMS ARS V 2.0	MARS-E V 2.0
RA-1	Risk Assessment Policy and Procedures	RA-1	RA-1	RA-1	RA-1
RA-2	Security Categorization	RA-2	RA-2	RA-2	RA-2
RA-3	Risk Assessment	RA-3	RA-3	RA-3	RA-3
RA-4	**Withdrawn**		---		
RA-5	Vulnerability Scanning	RA-5 (1)	RA-5 (1) (2) (5)	RA-5 (1) (2) (3) (5) (6)	RA-5 (1) (2) (3) (5)
RA-6	Technical Surveillance Countermeasures Survey		Not Selected		

Table 17. SA Family Controls Selection

Control No.	Control Name	MARS-EV 1.0	800-53 Rev 4 MODERATE BASELINE	CMS ARS V 2.0	MARS-E V 2.0
SA-1	System and Services Acquisition Policy and Procedures	SA-1	SA-1	SA-1	SA-1
SA-2	Allocation of Resources	SA-2	SA-2	SA-2	SA-2
SA-3	System Development Life Cycle	SA-3	SA-3	SA-3	SA-3
SA-4	Acquisition Process	SA-4 (1) (4)	SA-4 (1) (2) (9) (10)	SA-4 (1) (2) (7) (9) (10)	SA-4 (1) (2) (9)
SA-5	Information System Documentation	SA-5 (1) (3)	SA-5	SA-5	SA-5
SA-6	**Withdrawn**	SA-6	---		
SA-7	**Withdrawn**	SA-7	---		
SA-8	Security Engineering Principles	SA-8	SA-8	SA-8	SA-8
SA-9	External Information System Services	SA-9	SA-9 (2)	SA-9 (1) (2)	SA-9 (1) (2) (5)
SA-10	Developer Configuration Management	SA-10	SA-10	SA-10	SA-10
SA-11	Developer Security Testing and Evaluation	SA-11	SA-11	SA-11 (1)	SA-11 (1)

Control No.	Control Name	MARS-EV 1.0	800-53 Rev 4 MODERATE BASELINE	CMS ARS V 2.0	MARS-E V 2.0
SA-12	Supply Chain Protection		Not Selected	SA-12	
SA-13	Trustworthiness		Not Selected		
SA-14	Criticality Analysis		Not Selected		
SA-15	Development Process, Standards, and Tools		Not Selected		
SA-16	Developer-Provided Training		Not Selected		
SA-17	Developer Security Architecture and Design		Not Selected		
SA-18	Tamper Resistance and Detection		Not Selected		
SA-19	Component Authenticity		Not Selected		
SA-20	Customized Development of Critical Components		Not Selected		
SA-21	Developer Screening		Not Selected		
SA-22	Unsupported System Components		Not Selected		SA-22

Table 18. SC Family Controls Selection

Control No.	Control Name	MARS-EV 1.0	800-53 Rev 4 MODERATE BASELINE	CMS ARS V 2.0	MARS-E V 2.0
SC-1	System and Communications Protection Policy and Procedures	SC-1	SC-1	SC-1	SC-1
SC-2	Application Partitioning	SC-2	SC-2	SC-2	SC-2
SC-3	Security Function Isolation		Not Selected		
SC-4	Information in Shared Resources	SC-4	SC-4	SC-4	SC-4
SC-5	Denial of Service Protection	SC-5	SC-5	SC-5	SC-5
SC-6	Resource Availability		Not Selected	SC-6	SC-6
SC-7	Boundary Protection	SC-7 (1) (2) (3) (4) (5) (6) (7)	SC-7 (3) (4) (5) (7)	SC-7 (3) (4) (5) (7) (8) (12) (13) (18)	SC-7 (3) (4) (5) (7) (8) (12) (13) (18)

Control No.	Control Name	MARS-EV 1.0	800-53 Rev 4 MODERATE BASELINE	CMS ARS V 2.0	MARS-E V 2.0
SC-8	Transmission Confidentiality and Integrity	SC-8 (1)	SC-8 (1)	SC-8 (1) (2)	SC-8 (1) (2)
SC-9	**Withdrawn**	SC-9 (1)	---		
SC-10	Network Disconnect	SC-10	SC-10	SC-10	SC-10
SC-11	Trusted Path		Not Selected	SC-11	
SC-12	Cryptographic Key Establishment and Management	SC-12	SC-12	SC-12 (2)	SC-12 (2)
SC-13	Cryptographic Protection	SC-13 (1)	SC-13	SC-13	SC-13
SC-14	**Withdrawn**	SC-14	---		
SC-15	Collaborative Computing Devices	SC-15 (1)	SC-15	SC-15 (1)	SC-15
SC-16	Transmission of Security Attributes		Not Selected		
SC-17	Public Key Infrastructure Certificates	SC-17	SC-17	SC-17	SC-17
SC-18	Mobile Code	SC-18	SC-18	SC-18	SC-18
SC-19	Voice Over Internet Protocol	SC-19	SC-19	SC-19	SC-19
SC-20	Secure Name /Address Resolution Service (Authoritative Source)	SC-20 (1)	SC-20	SC-20	SC-20
SC-21	Secure Name /Address Resolution Service (Recursive or Caching Resolver)		SC-21	SC-21	SC-21
SC-22	Architecture and Provisioning for Name/Address Resolution Service	SC-22	SC-22	SC-22	SC-22
SC-23	Session Authenticity	SC-23	SC-23	SC-23	SC-23
SC-24	Fail in Known State		Not Selected		
SC-25	Thin Nodes		Not Selected		
SC-26	Honeypots		Not Selected		
SC-27	Platform-Independent Applications		Not Selected		
SC-28	Protection of Information at Rest	SC-28	SC-28	SC-28	SC-28
SC-29	Heterogeneity		Not Selected		
SC-30	Concealment and Misdirection		Not Selected	SC-30	

Control No.	Control Name	MARS-EV 1.0	800-53 Rev 4 MODERATE BASELINE	CMS ARS V 2.0	MARS-E V 2.0
SC-31	Covert Channel Analysis		Not Selected		
SC-32	Information System Partitioning	SC-32	Not Selected	SC-32	SC-32
SC-33	**Withdrawn**		---		
SC-34	Non-Modifiable Executable Programs		Not Selected		
SC-35	Honeyclients		Not Selected		
SC-36	Distributed Processing and Storage		Not Selected		
SC-37	Out-of-Band Channels		Not Selected		
SC-38	Operations Security		Not Selected		
SC-39	Process Isolation		SC-39	SC-39	SC-39
SC-40	Wireless Link Protection		Not Selected		
SC-41	Port and I/O Device Access		Not Selected		
SC-42	Sensor Capability and Data		Not Selected		
SC-43	Usage Restrictions		Not Selected		
SC-44	Detonation Chambers		Not Selected		
SC-ACA-1	Electronic Mail	SC-ACA-1		SC-CMS-1	SC-ACA-1
SC-ACA-2	FAX Usage				SC-ACA-2
SC-CMS-2	Website Usage			SC-CMS-2	Not Applicable

Table 19. SI Family Controls Selection

Control No.	Control Name	MARS-E V 1.0	800-53 Rev 4 MODERATE BASELINE	CMS ARS V 2.0	MARS-E V 2.0
SI-1	System and Information Integrity Policy and Procedures	SI-1	SI-1	SI-1	SI-1
SI-2	Flaw Remediation	SI-2 (1) (2)	SI-2 (2)	SI-2 (1) (2)	SI-2 (1) (2)
SI-3	Malicious Code Protection	SI-3 (1) (2) (3)	SI-3 (1) (2)	SI-3 (1) (2)	SI-3 (1) (2)
SI-4	Information System Monitoring	SI-4 (1) (2) (4) (5) (6)	SI-4 (2) (4) (5)	SI-4 (1) (2) (4) (5)	SI-4 (1) (2) (4) (5) (14)

Control No.	Control Name	MARS-E V 1.0	800-53 Rev 4 MODERATE BASELINE	CMS ARS V 2.0	MARS-E V 2.0
SI-5	Security Alerts, Advisories, and Directives	SI-5	SI-5	SI-5	SI-5
SI-6	Security Function Verification		Not Selected	SI-6	SI-6
SI-7	Software, Firmware, and Information Integrity	SI-7 (1)	SI-7 (1) (7)	SI-7 (1) (7)	SI-7 (1) (7)
SI-8	Spam Protection	SI-8 (1)	SI-8 (1) (2)	SI-8 (1) (2)	SI-8 (1) (2)
SI-9	**Withdrawn**	SI-9	---		
SI-10	Information Input Validation	SI-10	SI-10	SI-10	SI-10
SI-11	Error Handling	SI-11	SI-11	SI-11	SI-11
SI-12	Information Handling and Retention	SI-12	SI-12	SI-12	SI-12
SI-13	Predictable Failure Prevention		Not Selected		
SI-14	Non-Persistence		Not Selected		
SI-15	Information Output Filtering		Not Selected		
SI-16	Memory Protection		SI-16		SI-16
SI-17	Fail-Safe Procedures		Not Selected		

Table 20. PM Family Controls Selection

Control No.	Control Name	MARS-E V 1.0	800-53 Rev 4 MODERATE BASELINE	CMS ARS V 2.0	MARS-E V 2.0
PM-1	Information Security Program Plan	PM-1	PM-1	PM-1	PM-1
PM-2	Senior Information Security Officer	PM-2	PM-2	PM-2	PM-2
PM-3	Information Security Resources	PM-3	PM-3	PM-3	PM-3
PM-4	Plan of Action and Milestones Process	PM-4	PM-4	PM-4	PM-4
PM-5	Information System Inventory	PM-5	PM-5	PM-5	PM-5
PM-6	Information Security Measures of Performance	PM-6	PM-6	PM-6	PM-6

Control No.	Control Name	MARS-E V 1.0	800-53 Rev 4 MODERATE BASELINE	CMS ARS V 2.0	MARS-E V 2.0
PM-7	Enterprise Architecture	PM-7	PM-7	PM-7	PM-7
PM-8	Critical Infrastructure Plan	PM-8	PM-8	PM-8	PM-8
PM-9	Risk Management Strategy	PM-9	PM-9	PM-9	PM-9
PM-10	Security Authorization Process	PM-10	PM-10	PM-10	PM-10
PM-11	Mission/Business Process Definition	PM-11	PM-11	PM-11	PM-11
PM-12	Insider Threat Program		PM-12	PM-12	PM-12
PM-13	Information Security Workforce		PM-13	PM-13	PM-13
PM-14	Testing, Training, and Monitoring		PM-14	PM-14	PM-14
PM-15	Contacts with Security Groups and Associations		PM-15	PM-15	PM-15
PM-16	Threat Awareness Program		PM-16	PM-16	PM-16

Appendix B. Crosswalk to 45 CFR §155.260

Table 21. Mapping of 45 CFR §155.260 to MARS-E Version 2.0 Security and Privacy Controls[4]

§155.260 Requirement	MARS-E Version 2.0 Security Controls	MARS-E Version 2.0 Privacy Controls
(**a) Creation, collection, use and disclosure** (1) "…the Exchange may only use or disclose such personally identifiable information to the extent such information is necessary	AC-6: Least Privilege	AP-2: Purpose Specification AR-3: Privacy Requirements for Contractors and Service Providers DM-3: Minimization of PII used in Testing, Training, and Research [partial match]
(a)(1)(i) For the Exchange to carry out the functions described in §155.200;	AC-6: Least Privilege	DM-1: Minimization of Personally Identifiable Information DM-1 (1): Locate / Remove / Redact / Anonymize PII DM-3 (1): Risk Minimization Techniques UL-1: Internal Use
(ii) For the Exchange to carry out other functions not described in paragraph (a)(1)(i) of this section, which the Secretary determines to be in compliance with section 1411(g)(2)(A) of the Affordable Care Act and for which an individual provides consent for his or her information to be used or disclosed; or	AC-6: Least Privilege	DM-1: Minimization of Personally Identifiable Information DM-1 (1): Locate / Remove / Redact / Anonymize PII DM-3 (1): Risk Minimization Techniques
(iii) For the Exchange to carry out other functions not described in paragraphs (a)(1)(i) and (ii) of this section, for which an individual provides consent for his or her information to be used or disclosed, and which the Secretary determines are in compliance with section 1411(g)(2)(A) of the Affordable Care Act under the following substantive and procedural requirements:	AC-21: Information Sharing	DM-1: Minimization of Personally Identifiable Information DM-1 (1): Locate / Remove / Redact / Anonymize PII DM-3 (1): Risk Minimization Techniques
(a)(1)(iii) (**A) Substantive requirements.** The Secretary may approve other uses and disclosures of personally identifiable information created or collected as described in paragraph (a)(1) of this section that are not described in paragraphs (a)(1)(i) or (ii) of this section, provided that HHS determines that the information will be used only for the purposes of and to the extent necessary in ensuring the efficient operation of the Exchange consistent with section 1411(g)(2)(A) of the Affordable Care Act,	AC-1: Policy and Procedures AC-6: Least Privilege AC-3 (9): Access Enforcement – Controlled Release AC-20: Use of External Information Systems AC-21: Information Sharing	AR-6: Privacy Reporting UL-1: Internal Use

[4] References to the relevant 45 CFR §155.260 paragraph have been inserted into the security and privacy controls that are highly significant to the HHS Regulation.

§155.260 Requirement	MARS-E Version 2.0 Security Controls	MARS-E Version 2.0 Privacy Controls
and that the uses and disclosures are also permissible under relevant law and policy. **(a)(1)(iii) (B) Procedural requirements for approval of a use or disclosure of personally identifiable information.** To seek approval for a use or disclosure of personally identifiable information created or collected as described in paragraph (a)(1) of this section that is not described in paragraphs (a)(1)(i) or (ii) of this section, the Exchange must submit the following information to HHS: (1) Identity of the Exchange and appropriate contact persons; (2) Detailed description of the proposed use or disclosure, which must include, but not necessarily be limited to, a listing or description of the specific information to be used or disclosed and an identification of the persons or entities that may access or receive the information; (3) Description of how the use or disclosure will ensure the efficient operation of the Exchange consistent with section 1411(g)(2)(A) of the Affordable Care Act; and (4) Description of how the information to be used or disclosed will be protected in compliance with privacy and security standards that meet the requirements of this section or other relevant law, as applicable.		
(a)(2) The Exchange may not create, collect, use, or disclose personally identifiable information unless the creation, collection, use, or disclosure is consistent with this section.	AC-6: Least Privilege	AC-6: Least Privilege AR-3: Privacy Requirements for Contractors and Service Providers DM-1: Minimization of Personally Identifiable Information DM-1 (1): Locate / Remove / Redact / Anonymize PII
(a)(3) The Exchange must establish and implement privacy and security standards that are consistent with the following principles:	N/A	AR-1: Governance and Privacy Program AP-2: Purpose Specification AR-3: Privacy Requirements for Contractors and Service Providers
(a)(3)(i) *Individual access.* Individuals should be provided with a simple and timely means to access and obtain their personally identifiable information in a readable form and format;	* Privacy issue	IP-2: Individual Access TR-3: Dissemination of Privacy Program Information

§155.260 Requirement	MARS-E Version 2.0 Security Controls	MARS-E Version 2.0 Privacy Controls
(a)(3)(ii) "*Correction.* Individuals should be provided with a timely means to dispute the accuracy or integrity of their personally identifiable information and to have erroneous information corrected or to have a dispute documented if their requests are denied"	* Privacy issue	AR-8: Accounting of Disclosures IP-2: Individual Access IP-3: Redress IP-4: Complaint Management IP-4 (1): Response Time TR-3: Dissemination of Privacy Program Information
(a)(3)(iii) "*Openness and transparency.* There should be openness and transparency about policies, procedures, and technologies that directly affect individuals and/or their personally identifiable information**"**	* Privacy issue	AR-6: Privacy Reporting [partial match] IP-1: Consent IP-1 (1): Mechanisms Supporting Itemized or Tiered Content IP-2: Individual Access TR-1: Privacy Notice TR-1 (1): Real or Layered Notice TR-2: System of Record Notices and Privacy Act Statements TR-2 (1): Public Website Publication [partial match] TR-3: Dissemination of Privacy Program Information UL-1: Internal Use
(a)(3)(iv) "*Individual choice*. Individuals should be provided a reasonable opportunity and capability to make informed decisions about the collection, use, and disclosure of their personally identifiable information"	* Privacy issue	AR-6: Privacy Reporting [partial match] IP-1: Consent IP-1 (1): Mechanisms Supporting Itemized or Tiered Content IP-2: Individual Access TR-1: Privacy Notice TR-1 (1): Real or Layered Notice TR-2: System of Record Notices and Privacy Act Statements TR-2 (1): Public Website Publication [partial match] TR-3: Dissemination of Privacy Program Information UL-1: Internal Use

§155.260 Requirement	MARS-E Version 2.0 Security Controls	MARS-E Version 2.0 Privacy Controls
(a)(3)(v) "*Collection, use, and disclosure limitations*. Personally identifiable information should be created, collected, used, and/or disclosed only to the extent necessary to accomplish a specified purpose(s) and never to discriminate inappropriately"	AC-6: Least Privilege	DM-1: Minimization of Personally Identifiable Information DM-1 (1): Locate / Remove / Redact / Anonymize PII UL-1: Internal Use
(a)(3)(vi) "*Data quality and integrity*. Persons and entities should take reasonable steps to ensure that personally identifiable information is complete, accurate, and up-to-date to the extent necessary for the person's or entity's intended purposes and has not been altered or destroyed in an unauthorized manner"	AC-3: Access Enforcement AU-2: Audit Events AU-3: Content of Audit Records AU-6: Audit Review, Analysis, and Reporting AU-10: Non-repudiation SC-8: Transmission Confidentiality and Integrity SC-8 (1): Cryptographic or Alternate Physical Protection SC-8 (2): Pre/Post Transmission Handling SC-28: Protection of Information at Rest SI-4: Information System Monitoring SI-7: Software, Firmware, and Information Integrity SI-7 (1): Integrity Checks SI-10: Information Input Validation	AR-8: Accounting of Disclosures DI-1: Data Quality DI-1 (1): Validate PII DI-1 (2): Revalidate PII
(a)(3)(vii) "Safeguards. Personally identifiable information should be protected with reasonable operational, administrative, technical, and physical safeguards to ensure its confidentiality, integrity, and availability and to prevent unauthorized or inappropriate access, use, or disclosure**"**	All MARS-E security controls	DM-1: Minimization of Personally Identifiable Information SE-1: Inventory of Personally Identifiable Information [partial match]
(a)(3)(viii) "Accountability. These principles should be implemented, and adherence assured, through appropriate monitoring and other means and methods should be in place to report and mitigate non-adherence and breaches."	AU-1: Audit and Accountability Policy and Procedures AU-2: Audit Events AU-2 (3): Reviews and Updates AU-6: Audit Review, Analysis, and Reporting AU 9: Protection of Audit Information AU-10: Non-repudiation AU-11: Audit Record Retention AU-12: Audit Generation AU-12 (1): System-Wide / Time-Correlated Audit Trail CA-7: Continuous Monitoring	AR-4: Privacy Monitoring and Auditing AR-5: Privacy Awareness and Training AR-6: Privacy Reporting AR-7: Privacy-Enhanced System Design and Development [partial match] DM-1 (1): Locate / Remove / Redact / Anonymize PII SE-2: Privacy Incident Response TR-3: Dissemination of Privacy Program Information

§155.260 Requirement	MARS-E Version 2.0 Security Controls	MARS-E Version 2.0 Privacy Controls
	All IR Controls RA-3: Risk Assessment RA-5: Vulnerability Scanning	
(a)(4) The Exchange must establish and implement operational, technical, administrative and physical safeguards…:	All MARS-E Security Controls	AR-1: Governance and Privacy Program AR-3: Privacy Requirements for Contractors and Service Providers DM-1: Minimization of Personally Identifiable Information DM-1 (1): Locate / Remove / Redact / Anonymize PII
(a)(4)(i) Ensure… "The confidentiality, integrity, and availability of personally identifiable information created, collected, used, and/or disclosed by the Exchange"	All MARS-E Security Controls	AR-2: Privacy Impact and Risk Assessment DI-1: Data Quality DI-1 (1): Validate PII DI-1 (2): Revalidate PII DI-2: Data Integrity and Data Integrity Board DM-3: Minimization of PII used in Testing, Training, and Research SE-1: Inventory of Personally Identifiable Information
(a)(4)(ii) Ensure… "Personally identifiable information is only used by or disclosed to those authorized to receive or view it"	AC-1: Access Control Policies and Procedures AC-3: Access Enforcement AC-6: Least Privilege IA: Identification and Authentication Controls SC-4: Information In Shared Resources SC-8: Transmission Confidentiality and Integrity	AR-2: Privacy Impact and Risk Assessment DM-3: Minimization of PII used in Testing, Training, and Research IP-1: Consent IP-1 (1): Mechanisms Supporting Itemized or Tiered Content UL-1: Internal Use UL-2: Information Sharing with Third Parties
(a)(4)(iii) Ensure … "Return information, as such term is defined by section 6103(b)(2) of the Code, is kept confidential under section 6103 of the Code"	MARS-E Security Controls supplemented by IRS Supplied Appendix	AR-2: Privacy Impact and Risk Assessment DM-3: Minimization of PII used in Testing, Training, and Research IP-1: Consent IP-1 (1): Mechanisms Supporting Itemized or Tiered Content

§155.260 Requirement	MARS-E Version 2.0 Security Controls	MARS-E Version 2.0 Privacy Controls
(a)(4)(iv) Ensure… "Personally identifiable information is protected against any reasonably anticipated threats or hazards to the confidentiality, integrity, and availability of such information"	RA-3: Risk Assessment All MARS-E Security Controls	AR-2: Privacy Impact and Risk Assessment DM-3: Minimization of PII used in Testing, Training, and Research IP-1: Consent IP-1 (1): Mechanisms Supporting Itemized or Tiered Content SE-1: Inventory of Personally Identifiable Information
(a)(4)(v) Ensure … "Personally identifiable information is protected against any reasonably anticipated uses or disclosures of such information that are not permitted or required by law"	AC-21: Information Sharing PS: Personnel Security Controls	AR-2: Privacy Impact and Risk Assessment DM-3: Minimization of PII used in Testing, Training, and Research IP-1: Consent IP-1 (1): Mechanisms Supporting Itemized or Tiered Content
(a)(4)(vi) Ensure … "Personally identifiable information is securely destroyed or disposed of in an appropriate and reasonable manner and in accordance with retention schedules"	MP: Media Protection Controls SI-12: Information Handling and Retention	AR-8: Accounting of Disclosures DM-2: Data Retention and Disposal DM-2 (1): System Configuration
(a)(5) "The Exchange must monitor, periodically assess, and update the security controls and related system risks to ensure the continued effectiveness of those controls."	CA-1: Security Assessment and Authorization Policies and Procedures CA-2: Security Assessments CA-7: Continuous Monitoring RA-3: Risk Assessment	AR-2: Privacy Impact and Risk Assessment AR-3: Privacy Requirements for Contractors and Service Providers AR-4: Privacy Monitoring and Auditing AR-6: Privacy Reporting [partial match]
(a)(6) "The Exchange must develop and utilize secure electronic interfaces when sharing personally identifiable information electronically."	AC-20: Use of External Information Systems CA-3: System Interconnections SC-8 (1): Cryptographic or alternative physical protection	AR-3: Privacy Requirements for Contractors and Service Providers

§155.260 Requirement	MARS-E Version 2.0 Security Controls	MARS-E Version 2.0 Privacy Controls
(**b) Application to non-Exchange entities.** (b)(1)Non-Exchange entities. A non-Exchange entity is any individual or entity that: (i) Gains access to personally identifiable information submitted to an Exchange; or (ii) Collects, uses, or discloses personally identifiable information gathered directly from applicants, qualified individuals, or enrollees while that individual or entity is performing functions agreed to with the Exchange.	SA-4: Acquisition Process	AR-1: Governance and Privacy Program AR-3: Privacy Requirements for Contractors and Service Providers
(b) (2) Prior to any person or entity becoming a non-Exchange entity, Exchanges must execute with the person or entity a contract or agreement that includes:	SA-9: External Information System Services SA 9 (1): Risk Assessments / Organizational Approvals AC-3 (9): Access Enforcement – Controlled Release PS-6: Access Agreements	UL-2: Information Sharing with Third Parties
(b) (2) (i) A description of the functions to be performed by the non-Exchange entity;	AC-6: Least Privilege	AR-2: Privacy Impact and Risk Assessment AR-3: Privacy Requirements for Contractors and Service Providers
(b) (2) (ii) A provision(s) binding the non-Exchange entity to comply with the privacy and security standards and obligations adopted in accordance with paragraph (b)(3) of this section, and specifically listing or incorporating those privacy and security standards and obligations;	SA-4: Acquisition Process SA-4 (2): Design / Implementation Information for Security Controls	AR-2: Privacy Impact and Risk Assessment AR-3: Privacy Requirements for Contractors and Service Providers
(b) (2) (iii) A provision requiring the non-Exchange entity to monitor, periodically assess, and update its security controls and related system risks to ensure the continued effectiveness of those controls in accordance with paragraph (a)(5) of this section;	CA-1: Security Assessment and Authorization Policies and Procedures CA-2 Security Assessments CA-7: Continuous Monitoring RA-3: Risk Assessment	AR-2: Privacy Impact and Risk Assessment AR-3: Privacy Requirements for Contractors and Service Providers
(b) (2) (iv) A provision requiring the non-Exchange entity to inform the Exchange of any change in its administrative, technical, or operational environments defined as material within the contract; and	CA-1: Security Assessment and Authorization Policies and Procedures CM-3: Configuration Change Control RA-3: Risk Assessment SA 4: Acquisition Process	AR-2: Privacy Impact and Risk Assessment AR-3: Privacy Requirements for Contractors and Service Providers

§155.260 Requirement	MARS-E Version 2.0 Security Controls	MARS-E Version 2.0 Privacy Controls
(b) (2) (v) A provision that requires the non-Exchange entity to bind any downstream entities to the same privacy and security standards and obligations to which the non-Exchange entity has agreed in its contract or agreement with the Exchange.	PS-7: Third-Party Personnel Security SA 4: Acquisition Process SA-9: External Information System Services AC-3 (9): Access Enforcement – Controlled Release	AR-2: Privacy Impact and Risk Assessment AR-3: Privacy Requirements for Contractors and Service Providers
(b) (3) When collection, use or disclosure is not otherwise required by law, the privacy and security standards to which an Exchange binds non-Exchange entities must: (i) Be consistent with the principles and requirements listed in paragraphs (a)(1) through (6) of this section, including being at least as protective as the standards the Exchange has established and implemented for itself in compliance with paragraph (a)(3) of this section;	Reference a(1) through (6) above	AR-3: Privacy Requirements for Contractors and Service Providers AR-4: Privacy Monitoring and Auditing UL-2: Information Sharing with Third Parties
(ii) Comply with the requirements of paragraphs (c), (d), (f), and (g) of this section; and	SA-4: Acquisition Process CA-7: Continuous Monitoring	AR-3: Privacy Requirements for Contractors and Service Providers AR-4: Privacy Monitoring and Auditing UL-2: Information Sharing with Third Parties
(iii) Take into specific consideration: (A) The environment in which the non-Exchange entity is operating; (B) Whether the standards are relevant and applicable to the non-Exchange entity's duties and activities in connection with the Exchange; and (C) Any existing legal requirements to which the non-Exchange entity is bound in relation to its administrative, technical, and operational controls and practices, including but not limited to, its existing data handling and information technology processes and protocols.	SA-4: Acquisition Process All Applicable MARS-E Controls: AC-1: Access Control Policy and Procedures AT-1: Security Awareness and Training Policy and Procedures AU-1: Audit and Accountability Policy and Procedures CA-1: Security Assessment and Authorization Policies and Procedures CM-1: Configuration Management Policy and Procedures CP-1: Contingency Planning Policy and Procedures IA-1: Identification and Authentication Policy and Procedures IR-1: Incident Response Policy and Procedures MA-1: System Maintenance Policy and Procedures	AR-3: Privacy Requirements for Contractors and Service Providers AR-4: Privacy Monitoring and Auditing UL-2: Information Sharing with Third Parties

§155.260 Requirement	MARS-E Version 2.0 Security Controls	MARS-E Version 2.0 Privacy Controls
	MP-1: Media Protection Policy and Procedures PE-1: Physical and Environmental Protection Policy and Procedures PL-1: Security Planning Policy and Procedures PS-1: Personnel Security Policy and Procedures RA-1: Risk Assessment Policy and Procedures SA-1: System and Services Acquisition Policy and Procedures SC-1: System and Communications Protection Policy and Procedures SI-1: System and Information Integrity Policy and Procedures	
(c) "Workforce compliance. The Exchange must ensure its workforce complies with the policies and procedures developed and implemented by the Exchange to comply with this section."	AT-2: Security Awareness Training AT-3: Role-Based Security Training PS-1: Personnel Security Policy and Procedures PS-6: Access Agreements PS-8: Personnel Sanctions	AR-1: Governance and Privacy Program AR-3: Privacy Requirements for Contractors and Service Providers AR-4: Privacy Monitoring and Auditing AR-5: Privacy Awareness and Training UL-1: Internal Use [partial match]
(d) "Written policies and procedures. Policies and procedures regarding the creation collection, use, and disclosure of personally identifiable information must, at minimum: (1) Be in writing, and available to the Secretary of HHS upon request; and (2) Identify applicable law governing collection, use, and disclosure of personally identifiable information."	AC-1: Access Control Policy and Procedures	AP-1: Authority to Collect AR-1: Governance and Privacy program [partial match to "d(2)"] AR-3: Privacy Requirements for Contractors and Service Providers TR-3: Dissemination of Privacy Program Information

§155.260 Requirement	MARS-E Version 2.0 Security Controls	MARS-E Version 2.0 Privacy Controls
(e) "Data sharing. Data matching and sharing arrangements that facilitate the sharing of personally identifiable information between the Exchange and agencies administering Medicaid, CHIP or the BHP for the exchange of eligibility information must: (1) Meet any applicable requirements described in this section; (2) Meet any applicable requirements described in section 1413(c)(1) and (c)(2) of the Affordable Care Act; (3) Be equal to or more stringent than the requirements for Medicaid programs under section 1942 of the Act; and"	All MARS-E Security Controls	UL-2: Information Sharing with Third Parties DI-2 (1): Publish Agreements on Website
(e)(4) "For those matching agreements that meet the definition of "matching program" under 5 U.S.C. 552a(a)(8), comply with 5 U.S.C. 552a(o)."	AC-3 (9): Access Enforcement – Controlled Release	AR-8: Accounting of Disclosures [partial match] DI-1: Data Quality [partial match] DI-1 (2): Revalidate PII [partial match] DI-2: Data Integrity and Data Integrity Board DI-2 (1): Publish Agreements on Website
(f) "Compliance with the Code. Return information, as defined in section 6103(b)(2) of the Code, must be kept confidential and disclosed, used, and maintained only in accordance with section 6103 of the Code."	MARS-E Security Controls supplemented by IRS Appendix	AR-3: Privacy Requirements for Contractors and Service Providers DM-1: Minimization of Personally Identifiable Information [partial match] DM-1 (1): Locate / Remove / Redact / Anonymize PII UL-1: Internal Use [partial match]
(g) Improper use and disclosure of information. Any person who knowingly and willfully uses or discloses information in violation of section 1411(g) of the Affordable Care Act will be subject to a civil penalty of not more than $25,000 per person or entity, per use or disclosure, consistent with the bases and process for imposing civil penalties specified at §155.285, in addition to other penalties that may be prescribed by law.	PS-8: Personnel Sanctions	AR-3: Privacy Requirements for Contractors and Service Providers AR-4: Privacy Monitoring and Auditing

Master List of Acronyms for MARS-E Document Suite

AC	Access Control, a Security Control family
ACA	Patient Protection and Affordable Care Act of 2010
AE	Administering Entity
AP	Authority and Purpose, a Privacy Control family
API	Application Programming Interface
APT	Advanced Persistent Threat
AR	Accountability, Audit, and Risk Management, a Privacy Control family
AT	Awareness and Training, a Security Control family
ATC	Authority to Connect
ATO	Authorization to Operate
AU	Audit and Accountability, a Security Control family
BHP	Basic Health Program
BIOS	Basic Input Output System
BPA	Blanket Purchase Agreement
CA	Security Assessment and Authorization, a Security Control family
CAG	Consensus Audit Guidelines
CAP	Corrective Action Plan
CCIIO	Center for Consumer Information and Insurance Oversight
CE	Control Enhancement
CFR	Code of Federal Regulation
chown	Change Owner
CIO	Chief Information Officer
CIS	Center for Internet Security
CISO	Chief Information Security Officer
CM	Configuration Management, a Security Control family
CMA	Computer Matching Agreement
CMPPA	Computer Matching and Privacy Protection Act of 1988
CMS	Centers for Medicare & Medicaid Services
COTS	Commercial Off-the-Shelf
CP	Contingency Planning, a Security Control family

CTO	Chief Technology Officer
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
CWE	Common Weakness Enumeration
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DHS	Department of Homeland Security
DI	Data Quality and Integrity, a Privacy Control family
DISA	Defense Information Systems Agency
DM	Data Minimization and Retention, a Privacy Control family
DMZ	Demilitarized Zone
DNS	Domain Name System
DNSSEC	DNS Security
DoD	Department of Defense
DR	Disaster Recovery, a Security Control family
DSH	CMS Data Services Hub
DTR	Data Testing Report
EAP	Extensible Authentication Protocol
EHR	Electronic Healthcare Record
FDSH	Federal Data Services Hub
FFM	Federally-facilitated Marketplace
FIPPS	Fair Information Protection Principles
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
FTI	Federal Tax Information
FTP	File Transfer Protocol
GAGAS	Generally Accepted Governmental Auditing Standards
GMT	Greenwich Meridian Time
guid	Globally Unique Identifier
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 of 2009
HTTP	Hypertext Transfer Protocol
IA	Identification and Authentication, a Privacy Control family
ID	Identity
IDS	Intrusion Detection System
IEA	Information Exchange Agreement
IIHI	Individually Identifiable Health Information
IP	Internet Protocol
IP	Individual Participation and Redress, a Privacy Control family
IPS	Intrusion Prevention System
IR	Incident Response, a Privacy Control family
IRC	Internal Revenue Code
IRS	Internal Revenue Service
IS	Information Security
IS	Information System
ISA	Information Sharing Agreement
ISE	Information Sharing Environment
ISPG	Information Security Privacy Policy and Compliance Group
ISRA	Information Security Risk Assessment
IT	Information Technology
MA	Maintenance, a Security Control family
MAC	Media Access Control
MAGI	Modified Adjusted Gross Income
MARS-E	Minimum Acceptable Risk Standards for Exchanges
MFD	Multi-Function Device
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MP	Media Protection, a Security Control family
MTD	Maximum Tolerable Downtime
NARA	National Archives and Records Administration
NEE	Non-Exchange Entity
NIAP	National Information Assurance Partnership

NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency/Internal Report
NVD	National Vulnerability Database
OEI	Office of Enterprise Information
OMB	Office of Management and Budget
OPM	Office of Personnel Management
OVAL	Open Vulnerability Assessment Language
PDA	Portable Digital Assistant
PDF	Portable Document Format
PE	Physical and Environmental Protection, a Security Control family
PEAP	Protected Extensible Authentication Protocol
PHI	Protected Health Information
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
PL	Planning, a Security Control family
PM	Program Management, a Security Control family
POA&M	Plan of Action & Milestones
PS	Personnel Security, a Security Control family
Pub	Publication
QHP	Qualified Health Plan
RA	Risk Assessment, a Security Control family
RTO	Recovery Time Objectives
RUNAS	Microsoft command (allowing user to run specific tools and programs with different permissions other than as provided by user's current logon)
SA	System and Services Acquisition, a Security Control family
SAN	Storage Area Network
SAOP	Senior Agency Office for Privacy
SBM	State-based Marketplace
SC	System and Communications Protection, a Security Control family
SCAP	Security Content Automation Protocol
SDLC	System Development Life Cycle

SE	Security, a Privacy Control family
sftp	Secured File Transfer Protocol
SI	System and Information Integrity, a Security Control family
SIA	Security Impact Analysis
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SMART	SBM Annual Reporting Tool
SNA	Systems Network Architecture (IBM)
SORN	System of Record Notice
SOW	Statement of Work
SP	Special Publication
SSA	Social Security Administration
SSH	Secure Shell
SSP	System Security Plan
SSR	Safeguard Security Report
su	Substitute User Change user ID or become superuser
suid	Set User ID
TCP	Transmission Control Protocol
TIGTA	Treasury Inspector General for Tax Administration
TLS	Transport Layer Security
TR	Transparency, a Privacy Control family
UHF	Ultra High Frequency
UL	Use Limitation, a Privacy Control family
URL	Universal Resource Locator
USB	Universal Serial Bus
US-CERT	United States Computer Emergency Response Team
USGCB	United States Government Configuration Baseline
UTC	Universal Time Coordinate
UUENCODE	Unix-to-Unix Encode
VA	Department of Veterans Affairs
VDI	Virtual Desktop Infrastructure
VHF	Very High Frequency

VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WAP	Wireless Access Point
WIDS/WIPS	Wireless Intrusion Detection/Prevention System
WORM	Write-Once-Read-Many

Master Glossary for MARS-E Document Suite

Administering Entity (AE)	Exchanges, whether federal or state, state Medicaid agencies, state Children's Health Insurance Program (CHIP) agencies, or state agencies administering the Basic Health Program (BHP), or an entity established under Section 1311 of the ACA.
Affordable Care Act (ACA)	The comprehensive health care reform law enacted in March 2010. The law was enacted in two parts: The Patient Protection and Affordable Care Act was signed into law on March 23, 2010 and was amended by the Health Care and Education Reconciliation Act on March 30, 2010. The name "Affordable Care Act" is used to refer to the final, amended version of the law. The law's official title is the Patient Protection and Affordable Care Act of 2010 (Public Law No. 111-148), as amended by the Health Care and Education Reconciliation Act of 2010 (Public Law No. 111-152) (collectively, the ACA).
Authority to Connect (ATC)	This term is used in the execution of the Interconnection Security Agreement (ISA) with CMS. An "Authority to Connect (ATC)" by CMS is required to activate a system-to-system connection to the Data Services Hub.
Basic Health Program (BHP)	An optional state basic health program established under Section 1331 of the ACA. The Basic Health Program provides states with the option to establish a health benefits coverage program for lower-income individuals as an alternative to Health Insurance Marketplace coverage under the Affordable Care Act. This voluntary program enables states to create a health benefits program for residents with incomes that are too high to qualify for Medicaid through Medicaid expansion in the Affordable Care Act, but are in the lower income bracket to be eligible to purchase coverage through the Marketplace.
Breach	Defined by Office of Management and Budget (OMB) Memorandum M-07-16, *Safeguarding and Responding to the Breach of Personally Identifiable Information*, May 22, 2007, as the compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, loss of control, or any similar term or phrase that refers to situations where persons other than authorized users or for an other than authorized purpose have access or potential access to personally identifiable information, whether physical or electronic.
Children's Health Insurance Program (CHIP)	CHIP is a state-run federal health insurance program for uninsured children up to age 19 in families with too much income to qualify for Medicaid (Medical assistance) and that cannot afford to

	purchase health insurance. The state program was established under Title XXI of the Social Security Act.
Computer Matching Agreement (CMA)	An agreement that an organization enters into in connection with a computer matching program to which the organization is a party. A CMA is required for any computerized comparison of two or more systems of records or a system of records of non-federal records for the purpose of (1) establishments or verifying eligibility or compliance with law and regulations of applicants or recipients/beneficiaries, or (2) recouping payments or overpayments. One purpose of such a program is to establish or verify the eligibility of, or continuing compliance with, statutory and regulatory requirements by, applicants for, recipients or beneficiaries of, participants in, or providers of services with respect to cash or in-kind assistance or payments under federal benefit programs.
Digital Identity	The electronic representation of a real-world entity, and is usually taken to represent the online equivalent of a real individual. This online equivalent of an individual participates in electronic transactions on behalf of the individual it represents. Typically, digital identities are established and represented in the form of a unique identifier, such as a User ID, to represent an individual during a transaction.
Fair Information Practice Principles (FIPP)	Eight principles that provide the basis for these privacy controls, and are rooted in the federal Privacy Act of 1974, §208 of the E-Government Act of 2002, and Office of Management and Budget policies. The principles are transparency; individual participation; purpose specification; data minimization; use limitation; data quality and integrity; security; and accountability and auditing. The FIPPs are designed to build public trust in the privacy practices of organizations, and to help organizations avoid tangible costs and intangible damages from privacy incidents. The FIPPs are recognized in the U.S. and internationally as a general framework for privacy. Marketplace privacy and security regulations at 45 CFR §155.260(a) (3) (i)-(viii) require that Marketplaces establish and implement privacy and security standards that are consistent with and align with the eight principles of the FIPPs.
Federal Tax Information (FTI)	Defined broadly by the Internal Revenue Service (IRS) as including, but not limited to, any information, besides the return itself, that IRS obtained from any source or developed through any means that relates to the potential liability of any person under the IRS Code for any tax, penalty, interest, fine, forfeiture, or other imposition or offense; information extracted from a return, including names of dependents or the location of a business; the taxpayer's name, address, and identification number; information

	collected by the IRS about any person's tax affairs, even if identifiers are deleted; whether a return was filed, is or will be examined, or subject to other investigation or processing; and information collected on transcripts of accounts (for more information, see IRS Code §6103).
Federally-Facilitated Marketplace (FFM)	A Marketplace established and operated within a state by the Department of Health and Human Services (HHS) and operated by CMS under Section 1321(c) (1) of the ACA.
Federal Data Services Hub (Hub or FDSH)	The CMS federally managed service to transmit data between federal and state Administering Entities and to interface with federal agency partners and data sources.
Health Insurance Exchange (HIX)	A governmental agency or non-profit entity that meets the applicable standards of this part and makes Qualified Health Plans (QHP) available to qualified individuals and/or qualified employers. Unless otherwise identified, this term includes an Exchange serving the individual market for qualified individuals and a Small Business Health Options Program (SHOP) serving the small group market for qualified employers, regardless of whether the Exchange is established and operated by a state (including a regional Exchange or subsidiary Exchange) or by HHS.
Identity Proofing	In the context of the ACA, refers to a process through which the Marketplace, state Medicaid agency, or state CHIP agency obtains a level of assurance regarding an individual's identity that is sufficient to allow access to electronic systems that include sensitive (i.e., Personally Identifiable Information) state and federal data.
Incident	Means a violation or imminent threat of violation of security policies, acceptable use policies, or standard security practices. Incident means the act of violating an explicit or implied security policy, which includes attempts (either failed or successful) to gain unauthorized access to a system or its data; unwanted disruption or denial of service; the unauthorized use of a system for the processing or storage of data; and changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent. Incidents include the loss of data through theft or device misplacement, loss or misplacement of hardcopy documents, and misrouting of mail, all of which may have the potential to put the data at risk of unauthorized access, use, disclosure, modification or destruction. While certain adverse events, (e.g., floods, fires, electrical outages, and excessive heat) can cause system crashes, they are not considered incidents. An Incident becomes a Breach when there is the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations

	where persons other than authorized users and for an other than authorized purpose have access to personally identifiable information or personal health information, whether physical or electronic.
Information Exchange Agreement (IEA)	Agreement with CMS documenting the terms, conditions, safeguards, and procedures for exchanging information, when the information exchange is not covered by a computer matching agreement.
Information Security Risk Assessment (ISRA)	An analysis performed to assess the risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or information systems. The Information Security Risk Assessment process is used to provide the Business Owners with the means to continuously identify and mitigate business and system risks throughout the life cycle of the system.
Insurance Affordability Program	Program under Title I of the ACA for the enrollment in qualified health plans offered through a Marketplace, including but not limited to, enrollment with Advanced Premium Tax Credits (APTC) and Cost Sharing Reductions (CSR); (2) a State Medicaid program under Title XIX of the Social Security Act; (3) a state Children's Health Insurance Program (CHIP) under Title XXI of the Social Security Act; and (4) a state program under Section 1331 of the ACA establishing qualified basic health plans.
Interconnection Security Agreement (ISA)	Used for managing security risk exposures created by the interconnection of a system to another system owned by an external entity. Both parties agree to implement a set of common security controls. An "Authority to Connect (ATC)" by CMS is required to activate a system-to-system connection to the Data Services Hub.
IRS Safeguard Security Report (SSR)	Required by 26 U.S.C. §6103(p)(4)(E) and filed in accordance with IRS Publication 1075 to detail the safeguards established to maintain the confidentiality of Federal Tax Information (FTI) through the Hub or in an account transfer containing FTI.
Itemized Consent	See definition for Tiered Consent.
Layered Notice	A privacy notice approach that involves providing individuals with a summary of key points in the organization's privacy policy. A second notice provides more detailed and specific information.
Marketplace (or Exchange)	American Health Exchange established under Sections 1311(b), 1311(d), or 1321(c) (1) of the ACA, including both State-based Marketplaces (SBM) and Federally-Facilitated Marketplaces. The

	use of the term "Marketplace" in this Framework indicates that a control applies to both SBMs and FFMs.
Medicaid	The Medicaid program was established under Title XIX of the Social Security Act, together with other health care programs established under state law.
Multi-Factor Authentication (MFA)	Multi-factor authentication refers to the use of more than one of the following factors. The classic paradigm for authentication systems identifies three factors as the cornerstone of authentication: • Something you know (for example, a password) • Something you have (for example, an ID badge or a cryptographic key) • Something you are (for example, a fingerprint or other biometric data) The strength of authentication systems is largely determined by the number of factors incorporated by the system. Implementations that use two factors are considered to be stronger than those that use only one factor; systems that incorporate all three factors are stronger than systems that only incorporate two of the factors.
Non-Exchange Entity (NEE or Non-Marketplace Entity)	Also referred to as a "non-Exchange entity" (NEE) and as defined in regulation at 45 CFR §155.260(b), as, "any individual or entity that: (i) Gains access to personally identifiable information submitted to a Marketplace; or (ii) Collects, uses, or discloses personally identifiable information gathered directly from applicants, qualified individuals, or enrollees while that individual or entity is performing functions agreed to with the Marketplace. […]"
Personally Identifiable Information (PII)	As defined by National Institute of Standards and Technology (NIST) Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information."
Privacy Act Statement (PAS)	A notice that provides the authority of the Marketplace or Administering Entity to collect PII; whether providing PII is mandatory or optional; the principal purpose(s) for which the PII is to be used; the intended disclosure (routine uses) of the PII; and

	the consequences of not providing all, or some portion of, the PII requested.
Privacy Impact Assessment (PIA)	The process and document that is the outcome of the process of identifying privacy risks and methods to mitigate them. PIAs are performed before developing or procuring information systems, or initiating programs or projects that collect, use, maintain, or share PII, and they are updated when changes create new privacy risks. PIAs also are conducted to ensure that programs and information systems comply with applicable legal, regulatory, and policy requirements.
Real-time Notice	A privacy notice provided to the individual at the point of collection of information.
Qualified Health Plan (QHP)	Under the Affordable Care Act, an insurance plan that is certified by the health insurance Marketplace, provides essential health benefits, follows established limits on cost sharing (like deductibles, copayments, and out-of-pocket maximum amounts), and satisfies other requirements. A QHP has a certification by each Marketplace in which it is sold.
Qualified Individual	With respect to a Marketplace, an individual who has been determined eligible to enroll through the Marketplace in a qualified health plan in the individual market.
Remote Identity Proofing (RIDP)	Refers to a commonly used process to instantly identity proof the claimed identity of an individual over the Internet, such as an unknown visitor to an Administering Entity web portal.
Security Impact Analysis (SIA)	The analysis conducted by an organizational official to determine the extent to which changes to the information system have affected the security state of the system.
State-Based Marketplace (SBM)	As authorized by the Affordable Care Act, a health insurance Marketplace established and operated within a state, for which the state determines the specific criteria for plan certification and participation within broad federal regulations, and maintains local authority over managing health plans in the Marketplace.
State-Based Privacy and Security Artifacts	These are state-based privacy and security agreements to govern relationships where data sharing or system connections occur at the state level. All agreements at the state-level must bind the other party to meeting the same or more stringent privacy and security requirements than what is specified within 45 C.F.R. §155.260 (security standards are enumerated within the MARS-E Suite of documents). The state is responsible for the form these agreements take, such as contracts, Service Level Agreements, or memoranda of understanding.
System of Records	Defined in the Privacy Act at 5 U.S.C. §552a(a) (5). It is a group of any records under the control of any agency from which

	information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.
System of Records Notice (SORN)	A statement that provides public notice of the existence and character of a group of records under the control of any agency, from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual (for more information, see OMB Circular A-130, *Federal Agency Responsibilities for Maintaining Records About Individuals*).
System Security Plan (SSP)	As defined by NIST Special Publication Special Publication 800-37, an SSP is a formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements.
Tiered Consent	Also referred to as itemized consent, provides a means for individuals to authorize the collection, use, maintenance, and sharing of PII before its collection; provides a means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, or retention of PII; obtains individuals' consent to any new uses or disclosures of previously collected PII; and ensures that individuals are aware of and consent to all uses of PII not initially described in the public notice that was in effect at the time the organization collected the PII.

Master List of References for MARS-E Document Suite

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://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/
2. Security and Privacy Oversight and Monitoring Guide for Administering Entity (AE) Systems in Operation, available at: https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/
3. Change Reporting Procedures for State-Based Administering Entity Systems, available at: https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/
4. Framework for Independent Assessment of Security and Privacy Controls, available at: https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/
5. State-based Marketplace (SBM) IT Decommissioning and Data Retention Planning, available at: https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/
6. Administering Entity Security and Privacy Incident Report template , available at: https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/
7. Fed2NonFed Interconnection Security Agreement template, available at: https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/
8. State Plan of Action and Milestones, Template, available at: https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/
9. Information Security Risk Assessment (IS RA) Template Instructions, available at: https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/
10. Affordable Care Act Health Insurance Administering Entity Privacy Impact Assessment (PIA) template and guide, available at: https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/
11. Information Exchange Agreement Template, available at: https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/
12. Computer Matching Agreement (CMA) between CMS and State-Based Administering Entities, available at: https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/
13. Electronic Authentication Guidelines for ACA Administering Entity Systems, available at: https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/
14. MARS-E Security and Privacy Agreements and Compliance Artifacts briefing and supporting table, available at: https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/

Federal Legislation, Guidance, and Regulations

15. Public Law 111–148, Patient Protection and Affordable Care Act, March 23, 2010, 124 Stat. 119, available at: http://www.gpo.gov/fdsys/pkg/PLAW-111publ148/content-detail.html http://www.healthreform.gov/health_reform_and_hhs.html
16. Public Law 74-271, Social Security Act, as amended, available at: http://www.ssa.gov/OP_Home/ssact/ssact.htm
17. 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.congress/gov/bill/93rd-congess/senate-bill/S 3418
18. Public Law 104-13, Paperwork Reduction Act of 1995, as amended, available at: http://www.fws.gov/policy/library/rgpl104-13.pdf
19. Public Law 108–173, Medicare Prescription Drug, Improvement, and Modernization Act of 2003 (MMA), SEC. 912: Requirements for Information Security for Medicare Administrative Contractors, available at: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ173.108.pdf
20. Code of Federal Regulations (CFR), Regulation 5 CFR Part 731 – Suitability, 5CFR731, available at: http://www.access.gpo.gov/nara/cfr/waisidx/5cfr731.html
21. United States Code Title 44, Chapter 33—Disposal of Records, available at: http://www.archives.gov/about/laws/disposal-of-records.html
22. *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
23. Office of Management and Budget (OMB), Memorandum M-07-16, *Safeguarding and Responding to the Breach of Personally Identifiable Information*, May 22, 2007.
24. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, August 2013, available at: http://csrc.nist/publications/nistpubs/800-53/sp800-53.pdf
25. NIST SP 800-53A Rev 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations*, December 2014, available at: http://csrc.nist/publications/nistpubs/800-53A/sp800-53A.pdf
26. NIST SP 800-63, Version 1.0.2, *Electronic Authentication Guidelines*, April 2006, available at: http://csrc.nist/publications/nistpubs/800-63/sp800.63.pdf.
27. NIST SP 800-66 Rev 1, *An Introductory Resource Guide for Implementing the HIPAA Security Rule*, October 2008, available at: https://csrc.nist/publications/nistpubs/800-66/sp800.66.pdf
28. NIST SP 800-145, *The NIST Definition of Cloud Computing*, September 2011 available at: http://csrc.nist./publications/nistpubs/800-145/SP800.145.pdf.
29. NIST SP 800-88 Revision 1, *Guidelines for Media Sanitization*, December 2014, a Available at: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf

30. Federal Information Processing Standards (FIPS) Publication (PUB) 199, *Standards for Security Categorization of Federal Information and Information Systems,* NIST, February 2004, available at: http://csrc.nist/publications/nist pubs/fips 200/fips 199.pdf

31. FIPS Publication (PUB) 200, *Minimum Security Requirements for Federal Information and Information Systems*, NIST, March 2006, available at: http://csrc.nist/publications/nist pubs/fips 200/fips 200.pdf

32. 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

Department of Health and Human Services Regulations

33. 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. Amendment(s) published March 11, 2014, in 79 FR 13837, available at: http://www.ecfr.gov/cgi-bin/text-idx?SID=0ff499c497231aa32147d03c31622e81&node=20140311y1.120