Centers for Medicare & Medicaid Services

Minimum Acceptable Risk Safeguards for Exchanges (MARS-E) Document Suite

Volume I: Harmonized Security and Privacy Framework

Version 2.2

February 23, 2021

Foreword

The Centers for Medicare & Medicaid Services (CMS) is responsible for implementing many provisions of the Patient Protection and Affordable Care Act of 2010 (hereafter referred to as the "Affordable Care Act" or "ACA"). Accordingly, CMS developed, assembled, and implemented a document suite of guidance, requirements, and templates known as the Minimum Acceptable Risk Standards for Exchanges (MARS-E) in accordance with the Agency's Information Security and Privacy programs. MARS-E provides guidance on the protection of security and privacy in the ACA program environment; addresses the mandates of the ACA, including regulations 45 CFR §§155.260 and 155.280; and applies to all ACA Administering Entities (AE).[1]

CMS has updated MARS-E periodically since its first publication in 2012 to ensure continued compliance with the regulatory environment. Version 2.0 in November 2015 was the most recent major update. In developing MARS-E v. 2.0, CMS relied on the *CMS Acceptable Risk Safeguards (ARS)* v. 2.0, as the basis for the security and privacy control requirements. The *CMS ARS* is based on National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev 4, *Security and Privacy Controls for Federal Information Systems and Organizations.* MARS-E v. 2.0 of the MARS-E Document Suite consisted of four volumes:

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

This Version 2.2 is an interim release that reflects the updates to security and privacy policies and standards guidance at the national, Department of Health and Human Services (HHS), and CMS levels since 2015. The next major release, MARS-E v. 3.0, will incorporate CMS's interpretation, tailoring, and implementation guidance for NIST 800-53 Rev 5.[2] This interim release updates the individual control specifications in MARS-E v. 2.2 to align with the most current federal, Department, and Agency policies and standards. The following updates are the most noteworthy:

- In compliance with Office of Management and Budget (OMB) Circular A-130's emphasis on the need to implement continuous monitoring of risks and vulnerabilities, MARS-E v. 2.2 introduced a new set of Information System Continuous Monitoring guidelines.
- HHS issued guidelines on the timeliness of remediation of uncovered security and privacy weaknesses. These requirements have been incorporated into MARS-E Security Controls CA-5, RA-5, and SI-2.

[1] "Administering Entity" means Exchanges, whether federal or state, state Medicaid agencies, Children's Health Insurance Program (CHIP) agencies, or state agencies administering the Basic Health Program.

[2] At the time of publication of MARS-E 2.2, NIST had just published NIST SP 800-53 Rev. 5, available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

- NIST introduced updated requirements for e-authentication in NIST SP 800-63 Release 3, *Digital Identity Guidelines*. These requirements informed the MARS-E v. 2.2 e-authentication requirements.
- Where appropriate, CMS updated MARS-E control specifications to reflect the wording of *CMS ARS v. 3.1*.

In addition, CMS considered the operational experience and feedback from ACA Administering Entities to change MARS-E content to improve usefulness in the AE environment. MARS-E v. 2.2 removes previous redundancies throughout the four volumes of MARS-E v. 2.0 by consolidating this content into two volumes as follows:

- Volume I: Harmonized Security and Privacy Framework (previously Volume I)
- Volume II: ACA Administering Entity System Security and Privacy Plan (previously Volumes II, III, and IV)

This *Harmonized Security and Privacy Framework* presents a high-level introduction to and definition of the CMS framework for managing the security and privacy of the information systems operated by ACA Administering Entities. The appendices in MARS-E v.2.0 Volume II, which provided background on the content of security and privacy controls, now appear as appendices in Volume I.

Information on the structure of the security and privacy control tables in the body of Volume II of MARS-E v2.0 now reside in Volume II of MARS-E v 2.2, along with the Security and Privacy Control tables and instructions on completing the System Security and Privacy Plan.

Any changes to the MARS-E document suite must be approved by the CMS Chief Information Officer and the CMS Chief Information Security Officer (CMS Senior Agency Official for Privacy).

George C. Hoffmann -S
Digitally signed by George C. Hoffmann -S
Date: 2021.05.25 14:44:43 -04'00'

Office of the Chief Information Officer Date
Centers for Medicare & Medicaid Services

Robert M. Wood -S
Digitally signed by Robert M. Wood -S
Date: 2021.05.24 14:43:41 -04'00'

Office of the Chief Information Security Officer Date
Centers for Medicare & Medicaid Services

Executive Summary

This *Harmonized Security and Privacy Framework* defines a structure for managing the security and privacy requirements of systems deployed to administer the provisions of the Affordable Care Act (ACA) that ensure affordable healthcare for all Americans. The centerpiece of the framework is the streamlined and tailored selection of security and privacy controls for Exchanges. The Security and Privacy controls specify applicable policies, standards, and procedures necessary for:

- Administering Entities to manage privacy and security risks in State-Based Exchange and Medicaid/Children’s Health Insurance Program (CHIP) environments
- Administering Entities to manage the responsibility to assure security and privacy for authorized data usage of ACA Personally Identifiable Information (PII)
- The Centers for Medicare & Medicaid Services (CMS) to define its responsibility for compliance oversight and monitoring.

CMS has established this framework on the ACA; Department of Health and Human Services (HHS) Regulations implementing the ACA; the Privacy Act; Federal Information Security Management Act of 2002, amended by the Federal Information Security Modernization Act of 2014 (FISMA); Office of Management and Budget (OMB) A-130 requirements of the federal government; and security and privacy guidance provided by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 4.

Record of Changes

Version Number	Date	Author / Owner	Description of Change
1.0	August 1, 2012	CMS	Version 1.0 for publication
2.0	November 10, 2015	CMS	Version 2.0 for publication
2.1	September 3, 2019	CMS	Version 2.1 for Internal CMS Use
2.1.9	November 30, 2020	CMS	Version 2.1.9 for Internal CMS Review
2.2	February 23, 2021	CMS	Version 2.2 for publication

Table of Contents

List of Figures

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 requirement for each state to develop its own Health Insurance Exchange. Exchanges serve as organized marketplaces that allow consumers and small businesses to quickly compare available plan options based on price, benefits, and services. By pooling consumers, reducing transaction costs, and increasing transparency, Exchanges create more efficient and competitive health insurance markets for individuals and small employers. Consumers seeking health insurance coverage can go to the Health Insurance Exchanges to obtain comprehensive information on coverage options currently available and make informed health insurance choices.

As described in Section 1411(g) of the Affordable Care Act, the confidentiality of applicant information is a primary consideration and applicant information may only be used for the purposes of, and to the extent necessary in, ensuring the efficient operation of the Exchange. The Department of Health and Human Services (HHS) has recognized the importance of incorporating security and privacy standards into the Health Insurance Exchange program. 45 CFR §155.260 serves as the cornerstone for protecting the privacy and security of Personally Identifiable Information (PII). It permits the collection, creation, use, and disclosure of PII only for the performance of the functions of Exchanges (per 45 CFR §155.200).

Section 155.260 (a)(3) requires Exchanges to establish and implement security and privacy standards consistent with the eight Fair Information Practice Principles (FIPP): (1) Individual Access; (2) Correction; (3) Openness and Transparency; (4) Individual Choice; (5) Collection, Use and Disclosure Limitations; (6) Data Quality and Integrity; (7) Safeguards; and (8) Accountability. Section 155.260 (e) requires agreements between Exchanges and agencies administering Medicaid, CHIP, or the Basic Health Program (BHP) for the exchange of eligibility information to meet any applicable requirements under §155.260.

HHS and CMS are responsible for providing guidance and oversight for the Exchanges and the functions they perform as well as the information technology (IT) systems that facilitate eligibility determinations, exemptions, and enrollment in insurance affordability programs. 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 the enrollment process, ACA Administering Entities (AE) must collect PII from applicants for healthcare coverage. For eligibility determination, data matches are made against federal data sources held by various state and federal agencies. Adopting strong security and privacy protections is therefore necessary to meet the regulatory requirements of the program and to establish public trust and confidence that their personal information will be protected.

Federal agencies that provide data for the Exchange program include the Internal Revenue Service (IRS), Social Security Administration (SSA), Department of Defense (DoD), Department of Homeland Security (DHS), Department of Veteran Affairs (VA), Office of Personnel Management (OPM), and Peace Corps. Each agency has unique data protection regulations and requirements. ACA Administering Entities and their contractors must adhere to the data safeguard requirements of the Internal Revenue Code (IRC), 26 U.S.C. §6103 (hereafter simply the “Tax Information Safeguarding Requirements”) and all corresponding security guidance as a condition of receiving Federal Tax Information (FTI). In addition, most, if not all, states also have statutes that protect, in varying degrees, the privacy of PII that is collected or created by a state agency.

Given the diversity of federal and state laws and regulations governing security and privacy that may apply, CMS has formulated this *Harmonized Security and Privacy Framework* to identify key standards and processes to support compliance with the current body of laws and regulations. Nothing in this document should be construed to eliminate the obligation for an Administering Entity to comply with the requirements of other applicable bodies of laws/regulations that apply to Administering Entities [i.e., Title XVIII and XIX for Medicaid/Children's Health Insurance Program (CHIP) agencies, and 26 U.S.C. §6103, Safeguards for Protecting Federal Tax Returns and Return Information]. Depending on the information processed, an Administering Entity's IT system may be required to meet additional security control requirements as mandated by specific sources, whether federal, state, legal, program, or accounting.

1.1 Purpose and Scope

This Harmonized Security and Privacy Framework defines the framework established by the Department for managing the security and privacy of systems deployed to administer the health insurance purchasing aspects of the Affordable Care Act. The scope covers all systems operated by ACA Administering Entities (namely, state Medicaid Agency, state CHIP, state BHP, or an Exchange). Volume II of the MARS-E document suite 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.

1.2 Audience

This document describes the HHS ACA security and privacy governance framework applicable to ACA Administering Entities and their business partners, ACA program overseers, other federal agencies, and supporting contractors.

2. ACA Security and Privacy Management: A Multi-tiered Framework

A common, comprehensive harmonized security and privacy framework answers two critical needs for the Health Insurance Exchange: improving efficiencies with how AEs specify and implement information systems security and privacy controls and facilitating compliance and oversight services. The greatest benefit of the framework is its efficacy in identifying the potential vulnerabilities and risks to PII used by the Exchanges and Non-Exchange Entities (NEE).

CMS is deploying a seven-tiered framework, as shown in Figure 1, for managing the administrative, operational, and technical aspects of security and privacy of ACA systems. The Minimum Acceptable Risk Standards (Tier 4) are central to the framework. These standards are founded on:

- Tier 1 – Federal Legislation and Executive Mandates
- Tier 2 – HHS ACA Regulations
- Tier 3 – Federal Regulations and Guidance
- Tier 4 – Minimum Acceptable Risk Standards for Administering Entities

Tiers 5, 6, and 7 are instrumental to implementing the Minimum Acceptable Risk Standards.

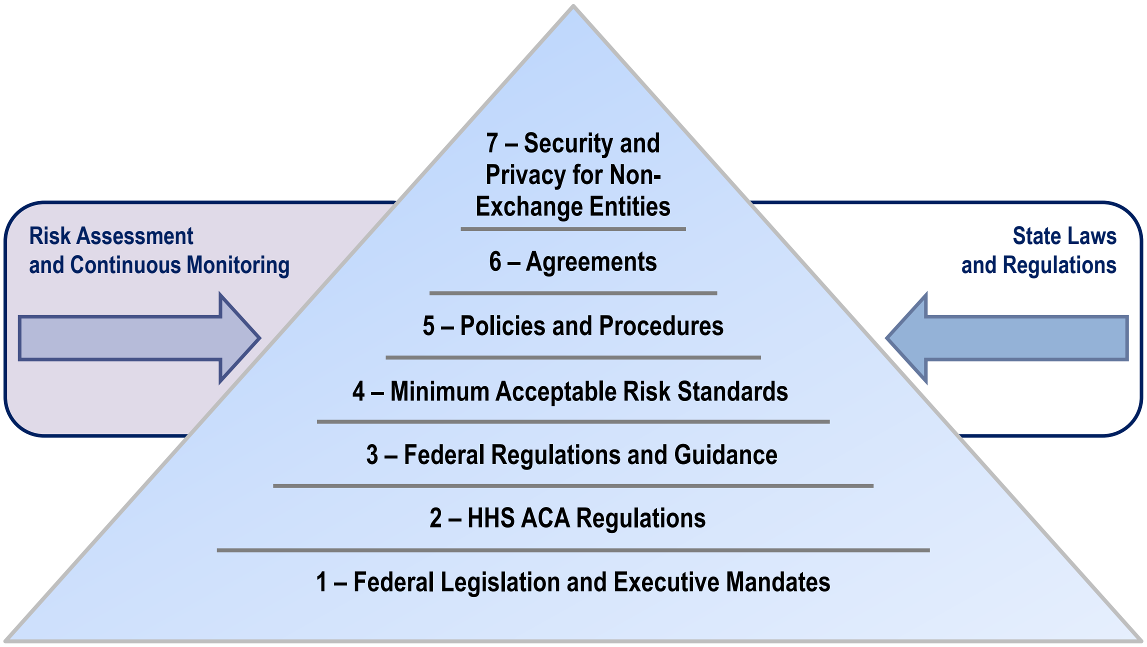
7 – Security and Privacy for Non-Exchange Entities
6 – Agreements
5 – Policies and Procedures
4 – Minimum Acceptable Risk Standards
3 – Federal Regulations and Guidance
2 – HHS ACA Regulations
1 – Federal Legislation and Executive Mandates
Risk Assessment and Continuous Monitoring
State Laws and Regulations

Figure 1. The ACA Security and Privacy Governance Framework

As depicted in Figure 1, two other factors must be considered when AEs establish the policy and standards for their own system environments: (1) state laws and regulations for security and privacy, and (2) outcomes of continuous monitoring and risk assessments of their own environment.

The following subsections address each tier of the Harmonized Security and Privacy Framework.

2.1 Tier 1 – Federal Laws and Executive Mandates

The landscape of security and privacy requirements presents a myriad of federal laws, regulations, guidance, and standards that may be difficult to navigate. Appendix A provides a brief overview of the key federal security and privacy laws that are essential to understanding the basic requirements levied on federal agencies, state partners, contractors, and supporting commercial companies. These include:

- Federal Information Security Management Act of 2002 amended by the Federal Information Security Modernization Act of 2014
- The Office of Management and Budget (OMB) revised Circular A-130 (2017), *Managing Information as a Strategic Resource*
- Privacy Act of 1974
- e-Government Act of 2002
- Patient Protection and Affordable Care Act of 2010
- HHS ACA Regulation
- Safeguards for Protecting Federal Tax Returns and Return Information (26 U.S.C. §6103 and related provisions)

2.1.1 Determining the Applicability of Federal Mandates

All federal agencies, and in some cases their contractors, must comply with FISMA, OMB Circular A-130, the Privacy Act of 1974, and the e-Government Act of 2002. Depending on the types of data created, collected, used, or disclosed, an AE system may need to comply with other federal mandates.

2.1.1.1 Data Types Requiring Special Protection

Table 1 provides the definitions for four types of data that require special protection.

Table 1. Key Data Definitions

Term	Definition
Personally Identifiable Information (PII)	As defined by OMB Memorandum M-17-12 (January 3, 2017), the term PII refers to 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.

Term	Definition
Individually Identifiable Health Information (IIHI)	HIPAA defines IIHI as any information, including demographic information collected from an individual, that (1) is created or received by a health care provider, health plan, employer, or health care clearinghouse, and relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (2) identifies the individual or where there is a reasonable basis to believe that the information can be used to identify the individual.
Protected Health Information (PHI)	Under HIPAA, PHI refers to individually identifiable health information that is maintained or transmitted by a covered entity or its business associate, in any form or medium, whether electronic, paper, or oral. There are certain exceptions such as for employment records held by a covered entity in its role as employer. PHI is considered a subset of PII.
Federal Tax Information (FTI)	Generally, federal tax returns and return information are confidential, as required by IRC §6103. The IRS enforces the IRC to ensure that agencies, bodies, and commissions maintain appropriate safeguards to protect information confidentiality. (See IRS Publication 1075 reference)

Because all Administering Entities process PII, controls required for the protection of PII have been incorporated into the MARS-E catalog. Controls required for other types of data have not been built into MARS-E. Each entity must perform an assessment of its own environment to determine what additional controls are needed.

IRC §6103 applies if an Administering Entity's IT system receives FTI. Please refer to Appendix A.6.3 for instructions.

Federal and non-federal organizations that operate Exchanges must determine their entity classification under HIPAA. Organizations must determine whether they are HIPAA covered entities or business associates. Covered entities are health plans, healthcare clearinghouses, and healthcare providers that transmit PHI electronically in connection with a HIPAA covered transaction. Business associates include persons, entities, or organizations that perform functions or services for or on behalf of HIPAA covered entities that involve the use or disclosure of PHI. Administering Entities that handle PHI are expected to implement the additional control requirements for PHI stated in the current *CMS Acceptable Risk Safeguards (CMS ARS)*.

2.2 Tier 2 – HHS ACA Regulations

Tier 2 of the framework is HHS's response to the ACA mandate: a set of HHS regulations stating how the department will discharge its responsibility in managing the security and privacy aspects of the Affordable Care Health Insurance Exchange program. On March 12, 2012, HHS issued the Final Rule on ACA Exchanges, §155.260 – Privacy and security of personally identifiable information. The Regulation was further revised on March 11, 2014.

On August 30, 2013, HHS published §155.280 – Oversight and monitoring of privacy and security requirements. This regulation provides HHS and Exchanges the authority to perform monitoring and oversight of subject entities. Section 155.280 also states that the Exchanges have the obligation to oversee and monitor Non-Exchange Entities in their compliance with privacy and security standards established by the state Exchange pursuant to §155.260. (Appendix A provides a summary of these regulations; the List of References provides citations to the source material.)

2.3 Tier 3 – Federal Regulations and Guidance

Tier 3 of the framework comprises the body of IT security and privacy regulations and guidance that form the technical backbone of MARS-E security and privacy control requirements. CMS has adopted the framework provided by 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,* and NIST SP 800-53A Rev 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans* in formulating this release of the security and privacy standards for ACA Administering Entities. Even though state-based AEs need not comply with FISMA, CMS has chosen NIST guidance as the basis for the standards for AEs because it is the *de facto* method for specifying security and privacy control requirements throughout the IT industry. Furthermore, the privacy control families in NIST SP 800-53 Rev 4 are congruent with the FIPPs principles contained in 45 CFR §155.260.

As a federal program, the ACA security and privacy program follows the federal mandates stated in Tier 1 of the framework. Implementations guidance for these mandates are reflected in the policies and standards issued HHS and CMS. Security guidance for systems operating in the cloud environment are issued by Federal Risk and Authorization Management Program (FedRAMP). The selection of controls presented in MARS-E v. 2.2, Volume II, Part B – Security and Privacy Controls Implementation, as shown in Appendix B, are based on *CMS ARS v. 3.1* (which is driven by HHS Information Policy for Security and Privacy), ACA Security and Privacy Regulations, and FedRAMP guidance for cloud-based systems.

2.4 Tier 4 – Minimum Acceptable Risk Standards

Tier 4, the Minimum Acceptable Risk Standards are documented in MARS-E v. 2.2, Volume II, Part B – Security and Privacy Controls Implementation. CMS developed the security and privacy controls 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.

Through this comprehensive selection of controls in Part B, CMS identifies the essential set of security and privacy controls that must be adopted by all entities implementing and operating an Exchange and/or Medicaid, CHIP, and Basic Health Program ACA health insurance purchasing systems. CMS established these MARS-E standards based on the Agency's interpretation of applicability of Tier 1, Tier 2, and Tier 3 mandates/guidance (as well as the applicability of HHS and CMS internal policies and guidance) to the ACA AE systems environment. The AEs must implement these controls in conjunction with requirements from other sources mandated for their systems environments.

The ACA security and privacy controls are 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.

2.4.1 Security Guidance

The security controls 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. Appendix B demonstrates how the MARS-E v. 2.2 security and privacy controls differ from those described in MARS-E v. 2.0 and the NIST 800-53 Rev 4 Moderate Baseline set. Volume II contains the following Security Control families:

- Access Control (AC)
- Awareness and Training (AT)
- Audit and Accountability (AU)
- Security Assessment and Authorization (CA)
- Configuration Management (CM)
- Contingency Planning (CP)
- Identification and Authentication (IA)
- Incident Response (IR)
- Maintenance (MA)
- Media Protection (MP)
- Physical and Environmental Protection (PE)
- Planning (PL)
- Personnel Security (PS)
- Risk Assessment (RA)
- System and Services Acquisition (SA)
- System and Communications Protection (SC)
- System and Information Integrity (SI)
- Program Management (PM)

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) to ensure 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.

The ACA law, HHS ACA Regulations, and CMS policy and standards form the basis of Administering Entity IT system security requirements. Table 23 provides 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.

2.4.2 Privacy Guidance

Building appropriate privacy protections into the design of the Exchanges 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 specific circumstances under which that information can be shared.

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 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's commitment to incorporate the FIPPs into the framework of the Health Insurance Exchanges program. 45 CFR §155.260(a)(3) identifies the eight privacy principles that form the basis on which all Exchanges must 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.

To secure PII in accordance with the ACA, the Catalog contains the following Privacy C families:

- Authority and Purpose (AP)
- Accountability, Audit and Risk Management (AR)
- Data Quality and Integrity (DI)
- Data Minimization and Retention (DM)
- Individual Participation and Redress (IP)
- Security (SE)
- Transparency (TR)
- Use Limitation (UL)

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.

2.5 Tier 5 – Policies, Guidance, and Procedures

Tier 5 of the MARS-E framework encompasses the set of policies, guidance, and procedures that support the implementation of required security and privacy controls. CMS has documented agency policies, guidance, and procedures for the technical areas of MARS-E implementation as well as CMS's oversight and monitoring for MARS-E compliance. CMS maintains a library of guidance and procedure documents in The Opportunity to Network and Exchange (zONE). For certain security and privacy controls, Implementation Standards have been modified or added to link to specific CMS implementation guidance documents that reside in the CMS ACA security and privacy implementation guidance repository.

The zONE platform is an online platform for organizations and individuals partnering and working with CMS on ACA Exchange-related matters. It is a secure, collaborative venue for such stakeholders as states, issuers, federal partners, business teams, and technology teams to connect, communicate, and share information including reusable documents, resources, and best practices.

2.6 Tier 6 – Use of Agreements (CMA, IEA, ISA, DUA)

Tier 6 of the framework is the body of legal agreements CMS uses to communicate conditions for sharing ACA PII and the associated security and privacy protection obligations. A large network of entities takes part in the administration of ACA health insurance eligibility determination, enrollment, and other Exchange functions. Each of the PII data-sharing instances carries obligations for ensuring authorized use and protecting the security and privacy of the shared data based on owner entity specifications. Obligations are communicated in the form of binding agreements (legal and/or data sharing). Data-sharing agreements include computer matching agreements (CMA), Information Exchange Agreements (IEA), and Data Use Agreements (DUA) that obligate the data-receiving entity to the security and privacy measures specified by the data-sharing entity.

An Interconnection Security Agreement (ISA) is required when data exchange takes place through the establishment of a system-to-system interconnection between the two parties. An ISA minimizes the security risk exposure on both sides, and ensures the confidentiality, integrity, and availability of the shared information as well as the network interconnection.

CMS executes CMAs, IEAs, and ISAs with its federal ACA PII data-sharing partners.

CMS executes similar agreements with state-based AEs. FISMA compliance is a requirement in all agreements with federal partners. When sharing data that originates from federal agencies, MARS-E compliance is a requirement in all CMS's data-sharing agreements with ACA AEs.

All AEs requesting interconnection to the Federal Data Services Hub (FDSH or Hub) for data sharing must demonstrate MARS-E compliance by submitting artifacts of security and privacy compliance as part of their ISA submission. The CMS CIO grants the Authority to Connect (ATC) upon review of the security and privacy compliance artifacts.

2.7 Tier 7 – Administering Entity Processes for Security and Privacy Governance of Non-Exchange Entities

To ensure the authorized collection, access, and disclosure of ACA PII by third parties with adequate control, Section155.260 (b) of the HHS Final Rule on ACA provides explicit requirements for data-sharing arrangements. Third parties, such as Agents or Brokers, also known as Non-Exchange Entities, must comply with all security and privacy standards established by HHS pursuant to 45 C.F.R. §155.260 related to the use of handling of PII. Administering Entities must execute NEE agreements with such NEEs to bind the downstream entity obtaining access to PII to the security and privacy standards for the use and disclosure of that information.

Furthermore, 45 C.F.R. §155.280 states that state Exchanges have the obligation to oversee and monitor Non-Exchange Entities in their compliance with privacy and security standards established by the state Exchange pursuant to §155.260.

2.8 Other Considerations

When faced with conflicting applicable federal and state requirements, Administering Entities must follow the most stringent requirement.

Appendix A. Key Laws and Guidance Governing Exchange of PII

There is no single federal law that governs all uses or disclosures of Personally Identifiable Information (PII). Instead, federal statutes provide privacy protections for information used for specific purposes or maintained by specific entities. The following subsections provide details on key laws as well as related regulations, standards, and guidance governing the exchange of PII. Entities that obtain access to Federal Tax Information (FTI) must look to the Internal Revenue Service (IRS) for guidance.

A.1 The Federal Information Security Management Act of 2002 and Its Amendment, the Federal Information Security Modernization Act of 2014

The Federal Information Security Modernization Act (FISMA) provides the primary statutory mandate governing information security in the federal government; it also addresses the protection of personal information in the context of securing federal agency information and information systems. FISMA establishes a risk-based approach to security management and defines federal requirements for securing information and information systems that support federal agency operations and assets. Under the Act, agencies are required to provide sufficient safeguards to cost effectively protect their information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction, including controls necessary to preserve authorized restrictions on access and disclosure (and thus to protect personal privacy, among other things). The Act also requires each agency to develop, document, and implement an agency-wide information security program to provide security for the information and information systems that support the operations and assets of the agency (including those provided or managed by another agency, contractor, or other source).

FISMA also establishes certain evaluation requirements. Under the Act, each agency must have an annual independent evaluation of its information security program and practices, including control testing and compliance assessment. Evaluations of non-national security systems are to be performed by the agency inspectors general or by an independent external auditor, while evaluations related to national security systems are to be performed only by an entity designated by the agency head.

Other major FISMA provisions require the National Institute for Standards and Technology (NIST) to develop, for systems other than national security systems, standards for categorizing information and information systems according to risk levels, guidelines on the types of information and information systems that should be included in each category, and standards for minimum information security requirements for information and information systems in each category. Accordingly, NIST developed the following guidance:

- **Federal Information Processing Standards (FIPS) Publication (Pub) 199,** ***Standards for Security Categorization of Federal Information and Information Systems*****.** This standard is to be used by all agencies to categorize all their information and information systems based on the objectives of providing appropriate levels of information security according to a range of risk levels. In addition, NIST has published Special Publication (SP) 800-60, *Guide for Mapping Types of Information and Information Systems to*

Security Categories, to provide guidance on how to implement FIPS Pub 199 and how to determine whether a system or information should be categorized as having a high-, moderate-, or low-risk impact level.

- **FIPS Pub 200, *Minimum Security Requirements for Federal Information and Information Systems*.** This standard provides minimum information security requirements for information and information systems in each risk category.
- **NIST SP 800-53 Rev 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.** This publication provides guidelines for selecting and specifying security controls for information systems supporting the federal government.
- **NIST SP 800-53A Rev 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*.** This publication provides the assessment procedures for security controls.

The Office of Management and Budget (OMB) is responsible for establishing government-wide policies and for providing guidance to agencies on how to implement the provisions of FISMA. For example, OMB requires that agency management officials formally authorize their information systems to process information and accept the risk associated with their operation. This management authorization is to be supported by a formal technical assessment of the controls established in an information system's security plan. In the wake of recent incidents of security breaches involving personal data, OMB has issued guidance reiterating the requirements of these laws and guidance, drawing particular attention to those associated with PII. In addition, OMB updated and added to requirements for reporting security breaches and the loss or unauthorized access of PII.

The Federal Information Security Modernization Act of 2014 amends the Federal Information Security Management Act of 2002 to: (1) reestablish the oversight authority of the Director of the OMB with respect to agency information security policies and practices, and (2) set forth authority for the Secretary of Homeland Security (DHS) to administer the implementation of such policies and practices for information systems. It provides for the use of automated tools in agencies' information security programs, including for periodic risk assessments, testing of security procedures, and detecting, reporting, and responding to security incidents.

Other federal laws may apply to sharing information with other entities, depending on the specific circumstances. Such laws may include the Freedom of Information Act of 1966 (FOIA), the Family Educational Rights and Privacy Act of 1974, and the Financial Modernization Act of 1999 (also known as Gramm-Leach-Bliley). Most, if not all, states also have statutes in place that, in varying degrees, protect the privacy of personal health information.

A.2 OMB Circular A-130

OMB issued a revised Circular A-130, *Managing Information as a Strategic Resource*, to reflect changes in law and advances in technology. The Circular establishes general policy for information governance, acquisitions, records management, open data, workforce, security, and privacy. It also emphasizes the role of both privacy and security in the federal information life cycle. Importantly, it represents a shift from viewing security and privacy requirements as compliance exercises to understanding security and privacy as crucial elements of a comprehensive, strategic, and continuous risk-based program at federal agencies.

A.3 The Privacy Act of 1974

The Privacy Act places limitations on the collection, disclosure, and use of personal information maintained in systems of records. The act describes a "record" as any item, collection, or grouping of information about an individual that is maintained by an agency and contains his or her name or another personal identifier. It also defines "system of records" as a group of records under the control of any agency from which information is retrieved by the name of the individual or by an individual identifier. The Privacy Act requires each agency that maintains a system of records to promulgate rules to meet the compliance requirements of the Privacy Act.

When agencies establish or make changes to a system of records, they must notify the public through a System of Records Notice (SORN) in the Federal Register that identifies, among other things, the categories of data collected, the categories of individuals about whom information is collected, the intended "routine" uses of data, and procedures that individuals can use to review and correct personally identifiable information. The act's requirements also apply to government contractors when agencies contract for the development and maintenance of a system of records to accomplish an agency function.

A computer matching program is required pursuant to The Computer Matching and Privacy Protection Act (CMPPA) of 1988 amending the Privacy Act for any computerized comparison of two or more automated systems of records, or a system of records with non-federal records, for the purpose of establishing or verifying eligibility or compliance as it relates to cash or in-kind assistance or payments under federal benefit programs [5 U.S.C. §552a(o)].

A.4 The e-Government Act of 2002

In 2002, Congress enacted the e-Government Act to enhance protection, among other things, for personal information in government information systems or information collections by requiring that agencies conduct a privacy impact assessment (PIA). A PIA is an analysis of how personal information is collected, stored, shared, and managed in a federal system. According to OMB guidance, a PIA is an analysis of how "… information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (ii) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks."

Agencies must conduct PIAs (1) before developing or procuring IT that collects, maintains, or disseminates information that is in identifiable form or (2) before initiating any new data collections of information in an identifiable form that will be collected, maintained, or disseminated using information technology (IT) if the same questions are asked of 10 or more people. OMB guidance also requires agencies to conduct PIAs when a system change creates new privacy risks, for example, changing the way in which personal information is used.

A.5 Patient Protection and Affordable Care Act of 2010

A.5.1 Section 1411(g) Confidentiality of Applicant Information

An applicant for insurance coverage shall be required to provide only the information strictly necessary to authenticate identity, determine eligibility, and determine the amount of the credit or reduction. Information collected shall only be used for Exchange operation.

A.6 HHS ACA Regulation

A.6.1 45 CFR §155.260 – Privacy and security of personally identifiable information

Part of the Department of Health and Human Services (HHS) regulation that specifies ACA standards for patient protection is 45 CFR §155.260 – Privacy and security of personally identifiable information issued on March 12, 2012. (An amendment was issued March 11, 2014). The regulation stipulates that the information collected either directly from an applicant or through other sources can only be used to perform the functions of an Exchange or as the Secretary determines is a function that ensures the efficient operation of the Exchange.

As a condition for processing PII associated with Exchange operations, the Exchanges must establish and implement privacy and security standards that address:

- Restricting the collection, creation, use and disclosure of PII to only the performance of the functions of Exchanges
- The eight privacy principles, which form the basis for security and privacy standards to safeguard PII
- Operational, technical, administrative, and physical safeguards that are consistent with applicable laws to prevent unauthorized or inappropriate access, use, or disclosure of PII
- Non-Exchange Entity use of PII
- Compliance with IRC provisions when an Administering Entity obtains FTI
- Civil penalty for any persons who willingly violate §1411(g) of the Affordable Care Act

The detailed contents of §155.260 can be found in Table 23 (Appendix B), which maps the §155.260 requirements to MARS-E 22, Security and Privacy Controls.

A.6.2 45 CFR §155.280 – Oversight and monitoring of privacy and security requirements

45 CFR §155.280 authorized HHS to oversee and monitor the Federally Facilitated Exchange and Non-Exchange Entities in their compliance with the privacy and security standards established and implemented by a Federally Facilitated Exchange pursuant to §155.260.

HHS will also oversee and monitor state Exchanges in their establishment and implementation of privacy and security standards pursuant to §155.260. The state Exchanges have the obligation to oversee and monitor Non-Exchange Entities in their compliance with privacy and security standards established by the state Exchange pursuant to §155.260.

As part of its oversight of compliance with the Exchange privacy and security standards, HHS may conduct audits, investigations, and inspections. HHS may also pursue civil, criminal or administrative proceedings or actions as determined necessary.

A.6.3 26 U.S.C. §6103, Safeguards for Protecting Federal Tax Returns and Return Information

Section 6103 of the Internal Revenue Code is a confidentiality statute and generally prohibits the disclosure of FTI; however, exceptions to the general rule authorize disclosure of FTI to certain federal, state, and local agencies. The Affordable Care Act authorizes the disclosure of FTI to assist Exchanges in the eligibility determination process.

As a condition of receiving FTI, the receiving State Administering Entity must show, to the satisfaction of the IRS, the ability to protect the confidentiality of that information. Safeguards must be designed to prevent unauthorized use, access, and disclosure and must ensure its safeguards will be ready for immediate implementation upon receipt of FTI. For more information, see *IRS Publication 1075 – Tax Information Security Guidelines for Federal, State, and Local Agencies* (http://www.irs.gov/pub/irs-pdf/p1075.pdf), and visit the IRS website at IRS.gov (keyword: safeguards) for additional guidance, job aids, helpful tools and frequently asked questions to assist agencies in meeting safeguard requirements.

Appendix B. MARS-E v. 2.2 Security Controls Selection Table

Table 1 through Table 19 show the security and privacy controls (and control enhancements) selected for the MARS-E v. 2.2 baseline (these are shown in the last column of the tables). These tables also report any differences with:

- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev4 MODERATE BASELINE
- Centers for Medicare & Medicaid Services (CMS) *Acceptable Risk Safeguards (ARS) v. 2.0*
- MARS-E v. 2.0
- Federal Risk and Authorization Management Program (FedRAMP) Moderate Baseline
- *CMS ARS v. 3.1* Non-cloud Baseline
- *CMS ARS v. 3.1* Cloud Baseline

Following the implementation of MARS-E v. 2.0, CMS learned that some Administering Entities (AE) operate in non-cloud environments. To accommodate this, CMS elected to identity cloud systems requirements separately in MARS-E v. 2.2 unlike MARS-E v. 2.0, where all cloud systems requirements were integrated into the baseline and implemented via a "one-size-fits-all" approach. Appendix C presents details on those changes.

Table 2. AC Family Controls Selection

Control No.	Control Name	800-53 Rev4 Moderate Baseline	CMS ARS v. 2.0	MARS-E v. 2.0	FedRAMP Moderate Baseline	CMS ARS v. 3.1 Moderate Baseline (Non-Cloud)	CMS ARS v. 3.1 Cloud Baseline	MARS-E v. 2.2
AC-1	Access Control Policy and Procedures	AC-1	AC-1	AC-1	AC-1	AC-1	AC-1	AC-1
AC-2	Account Management	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4) (7)	AC-2 (1) (2) (3) (4) (7)	AC-2 (1) (2) (3) (4) (5) (7) (9) (10) (12)	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4) (5) (7) (9) (10) (12)	AC-2 (1) (2) (3) (4) (5) (7) (9) (10) (12)
AC-3	Access Enforcement	AC-3	AC-3 (3)	AC-3 (9)	AC-3	AC-3	AC-3	AC-3 (9)
AC-4	Information Flow Enforcement	AC-4	AC-4	AC-4	AC-4 (21)	AC-4	AC-4 (21)	AC-4 (21)
AC-5	Separation of Duties	AC-5	AC-5	AC-5	AC-5	AC-5	AC-5	AC-5
AC-6	Least Privilege	AC-6 (1) (2) (5) (9) (10)	AC-6 (1) (2) (5) (9) (10)	AC-6 (1) (2) (5) (9) (10)	AC-6 (1) (2) (5) (9) (10)	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-7	AC-7	AC-7
AC-8	System Use Notification	AC-8	AC-8	AC-8	AC-8	AC-8	AC-8	AC-8
AC-9	Previous Logon (Access) Notification	Not Selected						
AC-10	Concurrent Session Control	Not Selected	AC-10	AC-10	AC-10		AC-10	AC-10
AC-11	Session Lock	AC-11 (1)	AC-11 (1)	AC-11 (1)	AC-11 (1)	AC-11 (1)	AC-11 (1)	AC-11 (1)
AC-12	Session Termination	AC-12	AC-12	AC-12	AC-12	AC-12	AC-12	AC-12
AC-13	Withdrawn	---	---					
AC-14	Permitted Actions without Identification or Authentication	AC-14 *(1) withdrawn	AC-14(1)	AC-14	AC-14	AC-14	AC-14	AC-14
AC-15	Withdrawn	---	---					
AC-16	Security Attributes	Not Selected	AC-16					
AC-17	Remote Access	AC-17 (1) (2) (3) (4)	AC-17 (1) (2) (3) (4)	AC-17 (1) (2) (3) (4)	AC-17 (1) (2) (3) (4) (9)	AC-17 (1) (2) (3) (4) (9)	AC-17 (1) (2) (3) (4) (9)	AC-17 (1) (2) (3) (4) (9)
AC-18	Wireless Access	AC-18 (1)	AC-18 (1)	AC-18 (1)	AC-18 (1)	AC-18 (1)	AC-18 (1)	AC-18 (1)
AC-19	Access Control for Mobile Devices	AC-19 (5)	AC-19 (5)	AC-19 (5)	AC-19 (5)	AC-19 (5)	AC-19 (5)	AC-19 (5)

Control No.	Control Name	800-53 Rev4 Moderate Baseline	CMS ARS v. 2.0	MARS-E v. 2.0	FedRAMP Moderate Baseline	CMS ARS v. 3.1 Moderate Baseline (Non-Cloud)	CMS ARS v. 3.1 Cloud Baseline	MARS-E v. 2.2
AC-20	Use of External Information Systems	AC-20 (1) (2)	AC-20 (1) (2)	AC-20 (1) (2)	AC-20 (1) (2)	AC-20 (1) (2)	AC-20 (1) (2)	AC-20 (1) (2) (3)
AC-21	Information Sharing	AC-21	AC-21	AC-21	AC-21	AC-21	AC-21	AC-21
AC-22	Publicly Accessible Content	AC-22	AC-22	AC-22	AC-22	AC-22	AC-22	AC-22

Table 3. AT Family Controls Selection

Control No.	Control Name	800-53 Rev4 Moderate Baseline	CMS ARS v. 2.0	MARS-E v. 2.0	FedRAMP Moderate Baseline	CMS ARS v. 3.1 Moderate Baseline (Non-Cloud)	CMS ARS v. 3.1 Cloud Baseline	MARS-E v. 2.2
AT-1	Security Awareness and Training Policy and Procedures	AT-1	AT-1	AT-1	AT-1	AT-1	AT-1	AT-1
AT-2	Security Awareness Training	AT-2 (2)	AT-2 (2)	AT-2 (2)	AT-2 (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-3	AT-3	AT-3
AT-4	Security Training Records	AT-4	AT-4	AT-4	AT-4	AT-4	AT-4	AT-4

Table 4. AU Family Controls Selection

Control No.	Control Name	800-53 Rev4 Moderate Baseline	CMS ARS v. 2.0	MARS-E v. 2.0	FedRAMP Moderate Baseline	CMS ARS v. 3.1 Moderate Baseline (Non-Cloud)	CMS ARS v. 3.1 Cloud Baseline	MARS-E v. 2.2
AU-1	Audit and Accountability Policy and Procedures	AU-1	AU-1	AU-1	AU-1	AU-1	AU-1	AU-1
AU-2	Audit Events	AU-2 (3)	AU-2 (3)	AU-2 (3)	AU-2 (3)	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-3 (1)	AU-3 (1)	AU-3 (1)
AU-4	Audit Storage Capacity	AU-4	AU-4	AU-4	AU-4	AU-4	AU-4	AU-4
AU-5	Response to Audit Processing Failures	AU-5	AU-5	AU-5 (1)	AU-5	AU-5	AU-5	AU-5

Control No.	Control Name	800-53 Rev4 Moderate Baseline	CMS ARS v. 2.0	MARS-E v. 2.0	FedRAMP Moderate Baseline	CMS ARS v. 3.1 Moderate Baseline (Non-Cloud)	CMS ARS v. 3.1 Cloud Baseline	MARS-E v. 2.2
AU-6	Audit Review, Analysis, and Reporting	AU-6 (1) (3)	AU-6 (1) (3)	AU-6 (1) (3)	AU-6 (1) (3)	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-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-8 (1)	AU-8 (1)	AU-8 (1)
AU-9	Protection of Audit Information	AU-9 (4)	AU-9 (2) (4)	AU-9 (4)	AU-9 (2) (4)	AU-9 (4)	AU-9 (2) (4)	AU-9 (2) (4)
AU-10	Non-repudiation	Not Selected	AU-10	AU-10	Not Selected			
AU-11	Audit Record Retention	AU-11	AU-11	AU-11	AU-11	AU-11	AU-11	AU-11
AU-12	Audit Generation	AU-12	AU-12 (1)	AU-12 (1)	AU-12	AU-12	AU-12	AU-12
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 5. CA Family Controls Selection

Control No.	Control Name	800-53 Rev4 Moderate Baseline	CMS ARS v. 2.0	MARS-E v. 2.0	FedRAMP Moderate Baseline	CMS ARS v, 3.1 Moderate Baseline (Non-Cloud)	CMS ARS v. 3.1 Cloud Baseline	MARS-E v. 2.2
CA-1	Security Assessment and Authorization Policies and Procedures	CA-1	CA-1	CA-1	CA-1	CA-1	CA-1	CA-1
CA-2	Security Assessments	CA-2 (1)	CA-2 (1)	CA-2 (1)	CA-2 (1) (2) (3)	CA-2 (1)	CA-2 (1) (2) (3)	CA-2 (1)
CA-3	System Interconnections	CA-3 (5)	CA-3 (5)	CA-3 (5)	CA-3 (3) (5)	CA-3 (3) (5)	CA-3 (3) (5)	CA-3 (3) (5)
CA-4	**Withdrawn**	---						
CA-5	Plan of Action and Milestones	CA-5	CA-5 (1)	CA-5 (1)	CA-5	CA-5	CA-5	CA-5
CA-6	Security Authorization	CA-6	CA-6	CA-6	CA-6	CA-6	CA-6	CA-6

Control No.	Control Name	800-53 Rev4 Moderate Baseline	CMS ARS v. 2.0	MARS-E v. 2.0	FedRAMP Moderate Baseline	CMS ARS v, 3.1 Moderate Baseline (Non-Cloud)	CMS ARS v. 3.1 Cloud Baseline	MARS-E v. 2.2
CA-7	Continuous Monitoring	CA-7 (1)	CA-7 (1)	CA-7 (1)	CA-7 (1)	CA-7 (1)	CA-7 (1)	CA-7 (1)
CA-8	Penetration Testing	Not Selected			CA-8 (1)		CA-8 (1)	CA-8 (1)
CA-9	Internal System Connections	CA-9	CA-9	CA-9	CA-9	CA-9	CA-9	CA-9

Table 6. CM Family Controls Selection

Control No.	Control Name	800-53 Rev4 Moderate Baseline	CMS ARS v. 2.0	MARS-E v. 2.0	FedRAMP Moderate Baseline	CMS ARS v. 3.1 Moderate Baseline (Non-Cloud)	CMS ARS v. 3.1 Cloud Baseline	MARS-E v. 2.2
CM-1	Configuration Management Policy and Procedures	CM-1	CM-1	CM-1	CM-1	CM-1	CM-1	CM-1
CM-2	Baseline Configuration	CM-2 (1) (3) (7)	CM-2 (1) (3) (7)	CM-2 (1) (3)	CM-2 (1) (2) (3) (7)	CM-2 (1) (3) (7)	CM-2 (1) (2) (3) (7)	CM-2 (1) (2) (3) (7)
CM-3	Configuration Change Control	CM-3 (2)	CM-3 (2)	CM-3 (2)	CM-3	CM-3 (2)	CM-3 (2)	CM-3 (2)
CM-4	Security Impact Analysis	CM-4	CM-4 (1) (2)	CM-4 (1) (2)	CM-4	CM-4 (2)	CM-4 (1) (2)	CM-4 (1) (2)
CM-5	Access Restrictions for Change	CM-5	CM-5 (1) (5)	CM-5 (1) (5)	CM-5 (1) (3) (5)	CM-5	CM-5 (1) (3) (5)	CM-5 (1) (3) (5)
CM-6	Configuration Settings	CM-6	CM-6 (1)	CM-6 (1)	CM-6 (1)	CM-6	CM-6 (1)	CM-6 (1)
CM-7	Least Functionality	CM-7 (1) (2) (4)	CM-7 (1) (2) (4)	CM-7 (1) (2) (4)	CM-7 (1) (2) (5)	CM-7 (1) (2) (4)	CM-7 (1) (2) (5)	CM-7 (1) (2) (5)
CM-8	Information System Component Inventory	CM-8 (1) (3) (5)	CM-8 (1) (3) (5)	CM-8 (1) (3) (5)	CM-8 (1) (3) (5)	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-9	CM-9	CM-9
CM-10	Software Usage Restrictions	CM-10	CM-10	CM-10 (1)	CM-10 (1)	CM-10	CM-10 (1)	CM-10 (1)
CM-11	User-Installed Software	CM-11	CM-11	CM-11	CM-11	CM-11	CM-11	CM-11

Table 7. CP Family Controls Selection

Control No.	Control Name	800-53 Rev4 Moderate Baseline	CMS ARS v. 2.0	MARS-E v. 2.0	FedRAMP Moderate Baseline	CMS ARS v. 3.1 Moderate Baseline (Non-Cloud)	CMS ARS v. 3.1 Cloud Baseline	MARS-E v. 2.2
CP-1	Contingency Planning Policy and Procedures	CP-1	CP-1	CP-1	CP-1	CP-1	CP-1	CP-1
CP-2	Contingency Plan	CP-2 (1) (3) (8)	CP-2 (1) (2) (3) (8)	CP-2 (1) (2) (3) (8)	CP-2 (1) (2) (3) (8)	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-3	CP-3	CP-3
CP-4	Contingency Plan Testing	CP-4 (1)	CP-4 (1)	CP-4 (1)	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-6 (1) (3)	CP-6 (1) (3)	CP-6 (1) (3)
CP-7	Alternate Processing Site	CP-7 (1) (2) (3)	CP-7 (1) (2) (3)	CP-7 (1) (2) (3)	CP-7 (1) (2) (3)	CP-7 (1) (2) (3)	CP-7 (1) (2) (3)	CP-7 (1) (2) (3)
CP-8	Telecommunications Services	CP-8 (1) (2)	CP-8 (1) (2)	CP-8 (1) (2)	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) (3)	CP-9 (1)	CP-9 (1) (3)	CP-9 (1)	CP-9 (1) (3)	CP-9 (1) (3)
CP-10	Information System Recovery and Reconstitution	CP-10 (2)	CP-10 (2)	CP-10 (2)	CP-10 (2)	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 8. IA Family Controls Selection

Control No.	Control Name	800-53 Rev4 Moderate Baseline	CMS ARS v. 2.0	MARS-E v. 2.0	FedRAMP Moderate Baseline	CMS ARS v. 3.1 Moderate Baseline (Non-Cloud)	CMS ARS v. 3.1 Cloud Baseline	MARS-E v. 2.2
IA-1	Identification and Authentication Policy and Procedures	IA-1	IA-1	IA-1	IA-1	IA-1	IA-1	IA-1
IA-2	Identification and Authentication (Organizational Users)	IA-2 (1) (2) (3) (8) (11) (12)	IA-2 (1) (2) (3) (8) (11) (12)	IA-2 (1) (2) (3) (8) (11)	IA-2 (1) (2) (3) (5) (8) (11) (12)	IA-2 (1) (2) (3) (8) (11) (12)	IA-2 (1) (2) (3) (5) (8) (11) (12)	IA-2 (1) (2) (3) (5) (8) (11)
IA-3	Device Identification and Authentication	IA-3	IA-3	IA-3	IA-3	IA-3	IA-3	IA-3
IA-4	Identifier Management	IA-4	IA-4	IA-4	IA-4 (4)	IA-4	IA-4 (4)	IA-4 (4)
IA-5	Authenticator Management	IA-5 (1) (2) (3) (11)	IA-5 (1) (2) (3) (6) (7) (11)	IA-5 (1) (2) (3) (7) (11)	IA-5 (1) (2) (3) (4) (6) (7) (11)	IA-5 (1) (2) (3) (11)	IA-5 (1) (2) (3) (4) (6) (7) (11)	IA-5 (1) (2) (3) (4) (6) (7) (11)
IA-6	Authenticator Feedback	IA-6	IA-6	IA-6	IA-6	IA-6	IA-6	IA-6
IA-7	Cryptographic Module Authentication	IA-7	IA-7	IA-7	IA-7	IA-7	IA-7	IA-7
IA-8	Identification and Authentication (Non-Organizational Users)	IA-8 (1) (2) (3) (4)	IA-8 (1) (2) (3) (4)	IA-8	IA-8 (1) (2) (3) (4)	IA-8 (1) (2) (3) (4)	IA-8 (1) (2) (3) (4)	IA-8 (2) (3) (4)
IA-9	Service Identification and Authentication	Not Selected						
IA-10	Adaptive Identification and Authentication	Not Selected						
IA-11	Re-authentication	Not Selected						

Table 9. IR Family Controls Selection

Control No.	Control Name	800-53 Rev4 Moderate Baseline	CMS ARS v. 2.0	MARS-E v. 2.0	FedRAMP Moderate Baseline	CMS ARS v. 3.1 Moderate Baseline (Non-Cloud)	CMS ARS v. 3.1 Cloud Baseline	MARS-E v. 2.2
IR-1	Incident Response Policy and Procedures	IR-1	IR-1	IR-1	IR-1	IR-1	IR-1	IR-1
IR-2	Incident Response Training	IR-2	IR-2	IR-2	IR-2	IR-2	IR-2	IR-2
IR-3	Incident Response Testing	IR-3 (2)	IR-3 (2)	IR-3 (2)	IR-3 (2)	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-4 (1)	IR-4 (1)	IR-4 (1)
IR-5	Incident Monitoring	IR-5	IR-5	IR-5	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-6 (1)	IR-6 (1)	IR-6 (1)
IR-7	Incident Response Assistance	IR-7 (1)	IR-7 (1) (2)	IR-7 (1)	IR-7 (1) (2)	IR-7 (1)	IR-7 (1) (2)	IR-7 (1) (2)
IR-8	Incident Response Plan	IR-8	IR-8	IR-8	IR-8	IR-8	IR-8	IR-8
IR-9	Information Spillage Response	Not Selected		IR-9	IR-9 (1) (2) (3) (4)		IR-9 (1) (2) (3) (4)	IR-9 (1) (2) (3) (4)
IR-10	Integrated Information Security Analysis Team	Not Selected						

Table 10. MA Family Controls Selection

Control No.	Control Name	800-53 Rev4 Moderate Baseline	CMS ARS v. 2.0	MARS-E v. 2.0	FedRAMP Moderate Baseline	CMS ARS v. 3.1 Moderate Baseline (Non-Cloud)	CMS ARS v. 3.1 Cloud Baseline	MARS-E v. 2.2
MA-1	System Maintenance Policy and Procedures	MA-1	MA-1	MA-1	MA-1	MA-1	MA-1	MA-1
MA-2	Controlled Maintenance	MA-2	MA-2	MA-2	MA-2	MA-2	MA-2	MA-2
MA-3	Maintenance Tools	MA-3 (1) (2)	MA-3 (1) (2) (3)	MA-3 (1) (2) (3)	MA-3 (1) (2) (3)	MA-3 (1) (2)	MA-3 (1) (2) (3)	MA-3 (1) (2) (3)
MA-4	Nonlocal Maintenance	MA-4 (2)	MA-4 (1) (2) (3)	MA-4 (1) (2) (3)	MA-4 (2)	MA-4 (1) (2)	MA-4 (2)	MA-4 (1) (2)
MA-5	Maintenance Personnel	MA-5	MA-5	MA-5	MA-5 (1)	MA-5	MA-5 (1)	MA-5 (1)
MA-6	Timely Maintenance	MA-6	MA-6	MA-6	MA-6	MA-6	MA-6	MA-6

Table 11. MP Family Controls Selection

Control No.	Control Name	800-53 Rev4 Moderate Baseline	CMS ARS v. 2.0	MARS-E v. 2.0	FedRAMP Moderate Baseline	CMS ARS v. 3.1 Moderate Baseline (Non-Cloud)	CMS ARS v. 3.1 Cloud Baseline	MARS-E v. 2.2
MP-1	Media Protection Policy and Procedures	MP-1	MP-1	MP-1	MP-1	MP-1	MP-1	MP-1
MP-2	Media Access	MP-2	MP-2	MP-2	MP-2	MP-2	MP-2	MP-2
MP-3	Media Marking	MP-3	MP-3	MP-3	MP-3	MP-3	MP-3	MP-3
MP-4	Media Storage	MP-4	MP-4	MP-4	MP-4	MP-4	MP-4	MP-4
MP-5	Media Transport	MP-5 (4)	MP-5 (4)	MP-5 (4)	MP-5 (4)	MP-5 (4)	MP-5 (4)	MP-5 (4)
MP-6	Media Sanitization	MP-6	MP-6 (1) (2)	MP-6 (1) (2)	MP-6 (2)	MP-6	MP-6 (1) (2)	MP-6 (1) (2)
MP-7	Media Use	MP-7 (1)	MP-7 (1)	MP-7 (1)	MP-7 (1)	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		MP-CMS-1

Table 12. PE Family Controls Selection

Control No.	Control Name	800-53 Rev4 Moderate Baseline	CMS ARS v. 2.0	MARS-E v. 2.0	FedRAMP Moderate Baseline	CMS ARS v. 3.1 Moderate Baseline (Non-Cloud)	CMS ARS v. 3.1 Cloud Baseline	MARS-E v. 2.2
PE-1	Physical and Environmental Protection Policy and Procedures	PE-1	PE-1	PE-1	PE-1	PE-1	PE-1	PE-1
PE-2	Physical Access Authorizations	PE-2	PE-2	PE-2 (1)	PE-2	PE-2	PE-2 (1)	PE-2 (1)
PE-3	Physical Access Control	PE-3	PE-3	PE-3	PE-3	PE-3	PE-3	PE-3
PE-4	Access Control for Transmission Medium	PE-4	PE-4	PE-4	PE-4	PE-4	PE-4	PE-4
PE-5	Access Control for Output Devices	PE-5	PE-5	PE-5	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-6(1)	PE-6 (1)	PE-6 (1)
PE-7	**Withdrawn**	---	---					

Control No.	Control Name	800-53 Rev4 Moderate Baseline	CMS ARS v. 2.0	MARS-E v. 2.0	FedRAMP Moderate Baseline	CMS ARS v. 3.1 Moderate Baseline (Non-Cloud)	CMS ARS v. 3.1 Cloud Baseline	MARS-E v. 2.2
PE-8	Visitor Access Records	PE-8	PE-8	PE-8	PE-8	PE-8	PE-8	PE-8
PE-9	Power Equipment and Cabling	PE-9	PE-9	PE-9	PE-9	PE-9	PE-9	PE-9
PE-10	Emergency Shutoff	PE-10	PE-10	PE-10	PE-10	PE-10	PE-10	PE-10
PE-11	Emergency Power	PE-11	PE-11	PE-11	PE-11	PE-11	PE-11	PE-11
PE-12	Emergency Lighting	PE-12	PE-12	PE-12	PE-12	PE-12	PE-12	PE-12
PE-13	Fire Protection	PE-13 (3)	PE-13 (1) (2) (3)	PE-13 (1) (2) (3)	PE-13 (2) (3)	PE-13 (3)	PE-13 (2) (3)	PE-13 (3)
PE-14	Temperature and Humidity Controls	PE-14	PE-14	PE-14	PE-14 (2)	PE-14	PE-14 (2)	PE-14
PE-15	Water Damage Protection	PE-15	PE-15	PE-15	PE-15	PE-15	PE-15	PE-15
PE-16	Delivery and Removal	PE-16	PE-16	PE-16	PE-16	PE-16	PE-16	PE-16
PE-17	Alternate Work Site	PE-17	PE-17	PE-17	PE-17	PE-17	PE-17	PE-17
PE-18	Location of Information System Components	Not Selected	PE-18	PE-18	Not Selected		Not Selected	
PE-19	Information Leakage	Not Selected						
PE-20	Asset Monitoring and Tracking	Not Selected						

Table 13. PL Family Controls Selection

Control No.	Control Name	800-53 Rev4 Moderate Baseline	CMS ARS v. 2.0	MARS-E v. 2.0	FedRAMP Moderate Baseline	CMS ARS v. 3.1 Moderate Baseline (Non-Cloud)	CMS ARS v. 3.1 Cloud Baseline	MARS-E v. 2.2
PL-1	Security Planning Policy and Procedures	PL-1	PL-1	PL-1	PL-1	PL-1	PL-1	PL-1
PL-2	System Security Plan	PL-2 (3)	PL-2 (3)	PL-2 (3)	PL-2 (3)	PL-2 (3)	PL-2 (3)	PL-2 (3)
PL-3	**Withdrawn**	---						
PL-4	Rules of Behavior	PL-4 (1)	PL-4 (1)	PL-4 (1)	PL-4 (1)	PL-4 (1)	PL-4 (1)	PL-4 (1)
PL-5	**Withdrawn**	---	--					

Control No.	Control Name	800-53 Rev4 Moderate Baseline	CMS ARS v. 2.0	MARS-E v. 2.0	FedRAMP Moderate Baseline	CMS ARS v. 3.1 Moderate Baseline (Non-Cloud)	CMS ARS v. 3.1 Cloud Baseline	MARS-E v. 2.2
PL-6	**Withdrawn**	---	--					
PL-7	Security Concept of Operations	Not Selected						
PL-8	Information Security Architecture	PL-8	PL-8	PL-8	PL-8	PL-8	PL-8	PL-8
PL-9	Central Management	Not Selected						

Table 14. PS Family Controls Selection

Control No.	Control Name	800-53 Rev4 Moderate Baseline	CMS ARS v. 2.0	MARS-E v. 2.0	FedRAMP Moderate Baseline	CMS ARS v. 3.1 Moderate Baseline (Non-Cloud)	CMS ARS v. 3.1 Cloud Baseline	MARS-E v . 2.2
PS-1	Personnel Security Policy and Procedures	PS-1	PS-1	PS-1	PS-1	PS-1	PS-1	PS-1
PS-2	Position Risk Designation	PS-2	PS-2	PS-2	PS-2	PS-2	PS-2	PS-2
PS-3	Personnel Screening	PS-3	PS-3	PS-3	PS-3 (3)	PS-3	PS-3 (3)	PS-3
PS-4	Personnel Termination	PS-4	PS-4	PS-4	PS-4	PS-4	PS-4	PS-4
PS-5	Personnel Transfer	PS-5	PS-5	PS-5	PS-5	PS-5	PS-5	PS-5
PS-6	Access Agreements	PS-6	PS-6	PS-6	PS-6	PS-6	PS-6	PS-6
PS-7	Third-Party Personnel Security	PS-7	PS-7	PS-7	PS-7	PS-7	PS-7	PS-7
PS-8	Personnel Sanctions	PS-8	PS-8	PS-8	PS-8	PS-8	PS-8	PS-8

Table 15. RA Family Controls Selection

Control No.	Control Name	800-53 Rev4 Moderate Baseline	CMS ARS v. 2.0	MARS-E v. 2.0	FedRAMP Moderate Baseline	CMS ARS v. 3.1 Moderate Baseline (Non-Cloud)	CMS ARS v. 3.1 Cloud Baseline	MARS-E v. 2.2
RA-1	Risk Assessment Policy and Procedures	RA-1	RA-1	RA-1	RA-1	RA-1	RA-1	RA-1
RA-2	Security Categorization	RA-2	RA-2	RA-2	RA-2	RA-2	RA-2	RA-2
RA-3	Risk Assessment	RA-3	RA-3	RA-3	RA-3	RA-3	RA-3	RA-3
RA-4	**Withdrawn**	---						
RA-5	Vulnerability Scanning	RA-5 (1) (2) (5)	RA-5 (1) (2) (3) (5) (6)	RA-5 (1) (2) (3) (5)	RA-5 (1) (2) (3) (5) (6) (8)	RA-5 (1) (2) (5)	RA-5 (1) (2) (3) (5) (6) (8)	RA-5 (1) (2) (3) (5) (6) (8)
RA-6	Technical Surveillance Countermeasures Survey	Not Selected						

Table 16. SA Family Controls Selection

Control No.	Control Name	800-53 Rev4 Moderate Baseline	CMS ARS v. 2.0	MARS-E v. 2.0	FedRAMP Moderate Baseline	CMS ARS v. 3.1 Moderate Baseline (Non-Cloud)	CMS ARS v. 3.1 Cloud Baseline	MARS-E v. 2.2
SA-1	System and Services Acquisition Policy and Procedures	SA-1	SA-1	SA-1	SA-1	SA-1	SA-1	SA-1
SA-2	Allocation of Resources	SA-2	SA-2	SA-2	SA-2	SA-2	SA-2	SA-2
SA-3	System Development Life Cycle	SA-3	SA-3	SA-3	SA-3	SA-3	SA-3	SA-3
SA-4	Acquisition Process	SA-4 (1) (2) (9) (10)	SA-4 (1) (2) (7) (9) (10)	SA-4 (1) (2) (9)	SA-4 (1) (2) (8) (9) (10)	SA-4 (1) (2) (8) (9) (10)	SA-4 (1) (2) (8) (9) (10)	SA-4 (1) (2) (8) (9)
SA-5	Information System Documentation	SA-5	SA-5	SA-5	SA-5	SA-5	SA-5	SA-5
SA-6	**Withdrawn**	---						
SA-7	**Withdrawn**	---						
SA-8	Security Engineering Principles	SA-8	SA-8	SA-8	SA-8	SA-8	SA-8	SA-8
SA-9	External Information System Services	SA-9 (2)	SA-9 (1) (2)	SA-9 (1) (2) (5)	SA-9 (1) (2) (4) (5)	SA-9 (1) (2) (4)	SA-9 (1) (2) (4) (5)	SA-9 (1) (2) (5)

Control No.	Control Name	800-53 Rev4 Moderate Baseline	CMS ARS v. 2.0	MARS-E v. 2.0	FedRAMP Moderate Baseline	CMS ARS v. 3.1 Moderate Baseline (Non-Cloud)	CMS ARS v. 3.1 Cloud Baseline	MARS-E v. 2.2
SA-10	Developer Configuration Management	SA-10	SA-10	SA-10	SA-10 (1)	SA-10	SA-10 (1)	SA-10 (1)
SA-11	Developer Security Testing and Evaluation	SA-11	SA-11 (1)	SA-11 (1)	SA-11 (1) (2) (8)	SA-11 (1)	SA-11 (1) (2) (8)	SA-11 (1) (2) (8)
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				SA-22

Table 17. SC Family Controls Selection

Control No.	Control Name	800-53 Rev4 Moderate Baseline	CMS ARS v. 2.0	MARS-E v. 2.0	FedRAMP Moderate Baseline	CMS ARS v. 3.1 Moderate Baseline (Non-Cloud)	CMS ARS v 3.1 Cloud Baseline	MARS-E v. 2.2
SC-1	System and Communications Protection Policy and Procedures	SC-1	SC-1	SC-1	SC-1	SC-1	SC-1	SC-1
SC-2	Application Partitioning	SC-2	SC-2	SC-2	SC-2	SC-2	SC-2	SC-2
SC-3	Security Function Isolation	Not Selected						

Control No.	Control Name	800-53 Rev4 Moderate Baseline	CMS ARS v. 2.0	MARS-E v. 2.0	FedRAMP Moderate Baseline	CMS ARS v. 3.1 Moderate Baseline (Non-Cloud)	CMS ARS v 3.1 Cloud Baseline	MARS-E v. 2.2
SC-4	Information in Shared Resources	SC-4	SC-4	SC-4	SC-4	SC-4	SC-4	SC-4
SC-5	Denial of Service Protection	SC-5	SC-5	SC-5	SC-5	SC-5	SC-5	SC-5
SC-6	Resource Availability	Not Selected	SC-6	SC-6	SC-6		SC-6	SC-6
SC-7	Boundary Protection	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)	SC-7 (3) (4) (5) (7) (8) (12) (13) (18)	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)
SC-8	Transmission Confidentiality and Integrity	SC-8 (1)	SC-8 (1) (2)	SC-8 (1) (2)	SC-8 (1)	SC-8 (1)	SC-8 (1)	SC-8 (1) (2)
SC-9	**Withdrawn**	---						
SC-10	Network Disconnect	SC-10	SC-10	SC-10	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 (2)	SC-12 (2)	SC-12 (2) (3)	SC-12	SC-12 (2) (3)	SC-12 (2) (3)
SC-13	Cryptographic Protection	SC-13	SC-13	SC-13	SC-13	SC-13	SC-13	SC-13
SC-14	**Withdrawn**	---						
SC-15	Collaborative Computing Devices	SC-15	SC-15 (1)	SC-15	SC-15	SC-15(1)	SC-15	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-17	SC-17	SC-17
SC-18	Mobile Code	SC-18	SC-18	SC-18	SC-18	SC-18	SC-18	SC-18
SC-19	Voice Over Internet Protocol	SC-19	SC-19	SC-19	SC-19	SC-19	SC-19	SC-19
SC-20	Secure Name /Address Resolution Service (Authoritative Source)	SC-20	SC-20	SC-20	SC-20	SC-20	SC-20	SC-20
SC-21	Secure Name /Address Resolution Service (Recursive or Caching Resolver)	SC-21	SC-21	SC-21	SC-21	SC-21	SC-21	SC-21

Control No.	Control Name	800-53 Rev4 Moderate Baseline	CMS ARS v. 2.0	MARS-E v. 2.0	FedRAMP Moderate Baseline	CMS ARS v. 3.1 Moderate Baseline (Non-Cloud)	CMS ARS v 3.1 Cloud Baseline	MARS-E v. 2.2
SC-22	Architecture and Provisioning for Name/Address Resolution Service	SC-22	SC-22	SC-22	SC-22	SC-22	SC-22	SC-22
SC-23	Session Authenticity	SC-23	SC-23	SC-23	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 (1)	SC-28 (1)	SC-28	SC-28 (1)
SC-29	Heterogeneity	Not Selected						
SC-30	Concealment and Misdirection	Not Selected	SC-30					
SC-31	Covert Channel Analysis	Not Selected						
SC-32	Information System Partitioning	Not Selected	SC-32	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-39	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						

Control No.	Control Name	800-53 Rev4 Moderate Baseline	CMS ARS v. 2.0	MARS-E v. 2.0	FedRAMP Moderate Baseline	CMS ARS v. 3.1 Moderate Baseline (Non-Cloud)	CMS ARS v 3.1 Cloud Baseline	MARS-E v. 2.2
SC-44	Detonation Chambers	Not Selected						
SC-ACA-1	Electronic Mail		SC-CMS-1	SC-ACA-1		SC-CMS-1		SC-ACA-1
SC-ACA-2	FAX Usage			SC-ACA-2		SC-CMS-2		SC-ACA-2
SC-CMS-2	Website Usage		SC-CMS-2	Not Applicable				

Table 18. SI Family Controls Selection

Control No.	Control Name	800-53 Rev4 Moderate Baseline	CMS ARS v. 2.0	MARS-E v. 2.0	FedRAMP Moderate Baseline	CMS ARS v. 3.1 Moderate Baseline (Non-Cloud)	CMS ARS v. 3.1 Cloud Baseline	MARS-E v. 2.2
SI-1	System and Information Integrity Policy and Procedures	SI-1	SI-1	SI-1	SI-1	SI-1	SI-1	SI-1
SI-2	Flaw Remediation	SI-2 (2)	SI-2 (1) (2)	SI-2 (1) (2)	SI-2 (2) (3)	SI-2 (2)	SI-2 (2) (3)	SI-2 (2)
SI-3	Malicious Code Protection	SI-3 (1) (2)	SI-3 (1) (2)	SI-3 (1) (2)	SI-3 (1) (2) (7)	SI-3 (1) (2)	SI-3 (1) (2) (7)	SI-3 (1) (2) (7)
SI-4	Information System Monitoring	SI-4 (2) (4) (5)	SI-4 (1) (2) (4) (5)	SI-4 (1) (2) (4) (5) (14)	SI-4 (1) (2) (4) (5) (14) (16 (23)	SI-4 (2) (4) (5)	SI-4 (1) (2) (4) (5) (14) (16 (23)	SI-4 (1) (2) (4) (5) (14) (16 (23)
SI-5	Security Alerts, Advisories, and Directives	SI-5	SI-5	SI-5	SI-5	SI-5	SI-5	SI-5
SI-6	Security Function Verification	Not Selected	SI-6	SI-6	SI-6		SI-6	SI-6
SI-7	Software, Firmware, and Information Integrity	SI-7 (1) (7)	SI-7 (1) (7)	SI-7 (1) (7)	SI-7 (1) (7)	SI-7 (1) (7)	SI-7 (1) (7)	SI-7 (1) (7)
SI-8	Spam Protection	SI-8 (1) (2)	SI-8 (1) (2)	SI-8 (1) (2)	SI-8 (1) (2)	SI-8 (1) (2)	SI-8 (1) (2)	SI-8 (1) (2)
SI-9	**Withdrawn**	---						
SI-10	Information Input Validation	SI-10	SI-10	SI-10	SI-10	SI-10	SI-10	SI-10
SI-11	Error Handling	SI-11	SI-11	SI-11	SI-11	SI-11	SI-11	SI-11
SI-12	Information Handling and Retention	SI-12	SI-12	SI-12	SI-12	SI-12	SI-12	SI-12
SI-13	Predictable Failure Prevention	Not Selected						
SI-14	Non-Persistence	Not Selected						

Control No.	Control Name	800-53 Rev4 Moderate Baseline	CMS ARS v. 2.0	MARS-E v. 2.0	FedRAMP Moderate Baseline	CMS ARS v. 3.1 Moderate Baseline (Non-Cloud)	CMS ARS v. 3.1 Cloud Baseline	MARS-E v. 2.2
SI-15	Information Output Filtering	Not Selected						
SI-16	Memory Protection	SI-16		SI-16	SI-16	SI-16	SI-16	SI-16
SI-17	Fail-Safe Procedures	Not Selected						

Table 19. PM Family Controls Selection

Control No.	Control Name	800-53 Rev4 Moderate Baseline	CMS ARS v. 2.0	MARS-E v. 2.0	FedRAMP Moderate Baseline	CMS ARS v. 3.1 Moderate Baseline (Non-Cloud)	CMS ARS v. 3.1 Cloud Baseline	MARS-E v. 2.2
PM-1	Information Security Program Plan	PM-1	PM-1	PM-1		PM-1	PM-1	PM-1
PM-2	Senior Information Security Officer	PM-2	PM-2	PM-2		PM-2	PM-2	PM-2
PM-3	Information Security Resources	PM-3	PM-3	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-4	PM-4
PM-5	Information System Inventory	PM-5	PM-5	PM-5		PM-5	PM-5	PM-5
PM-6	Information Security Measures of Performance	PM-6	PM-6	PM-6		PM-6	PM-6	PM-6
PM-7	Enterprise Architecture	PM-7	PM-7	PM-7		PM-7	PM-7	PM-7
PM-8	Critical Infrastructure Plan	PM-8	PM-8	PM-8		PM-8	PM-8	PM-8
PM-9	Risk Management Strategy	PM-9	PM-9	PM-9		PM-9	PM-9	PM-9
PM-10	Security Authorization Process	PM-10	PM-10	PM-10		PM-10	PM-10	PM-10
PM-11	Mission/Business Process Definition	PM-11	PM-11	PM-11		PM-11	PM-11	PM-11
PM-12	Insider Threat Program	PM-12	PM-12	PM-12		PM-12	PM-12	PM-12
PM-13	Information Security Workforce	PM-13	PM-13	PM-13		PM-13	PM-13	PM-13
PM-14	Testing, Training, and Monitoring	PM-14	PM-14	PM-14		PM-14	PM-14	PM-14

Control No.	Control Name	800-53 Rev4 Moderate Baseline	CMS ARS v. 2.0	MARS-E v. 2.0	FedRAMP Moderate Baseline	CMS ARS v. 3.1 Moderate Baseline (Non-Cloud)	CMS ARS v. 3.1 Cloud Baseline	MARS-E v. 2.2
PM-15	Contacts with Security Groups and Associations	PM-15	PM-15	PM-15		PM-15	PM-15	PM-15
PM-16	Threat Awareness Program	PM-16	PM-16	PM-16		PM-16	PM-16	PM-16

Table 20. Privacy Controls Selection

Control No.	Control Name	800-53 Rev4 Moderate Baseline	CMS ARS v. 2.0	MARS-E v. 2.0	FedRAMP Moderate Baseline	CMS ARS v. 3.1 Moderate Baseline (Non-Cloud)	CMS ARS v. 3.1 Cloud Baseline	MARS-E v. 2.2
AP-1	Authority to Collect			AP-1		AP-1	AP-1	AP-1
AP-2	Purpose Specification			AP-2		AP-2	AP-2	AP-2
AR-1	Governance and Privacy Program			AR-1		AR-1	AR-1	AR-1
AR-2	Privacy Impact and Risk Assessment			AR-2		AR-2	AR-2	AR-2
AR-3	Privacy Requirements for Contractors and Service Providers			AR-3		AR-3	AR-3	AR-3
AR-4	Privacy Monitoring and Auditing			AR-4		AR-4	AR-4	AR-4
AR-5	Privacy Awareness and Training			AR-5		AR-5	AR-5	AR-5
AR-6	Privacy Reporting					AR-6	AR-6	
AR-7	Privacy-enhanced System Design and Development			AR-7		AR-7	AR-7	AR-7
AR-8	Accounting of Disclosures			AR-8		AR-8	AR-8	AR-8
DI-1	Data Quality			DI-1 (1) (2)		DI-1 (1) (2)	DI-1 (1) (2)	DI-1 (1) (2)
DI-2	Data Integrity and Data Integrity Board					DI-2 (1)	DI-2 (1)	
DM-1	Minimization of Personally Identifiable Information			DM-1 (1)		DM-1 (1)	DM-1 (1)	DM-1 (1)
DM-2	Data Retention and Disposal			DM-2 (1)		DM-2 (1)	DM-2 (1)	DM-2 (1)

Control No.	Control Name	800-53 Rev4 Moderate Baseline	CMS ARS v. 2.0	MARS-E v. 2.0	FedRAMP Moderate Baseline	CMS ARS v. 3.1 Moderate Baseline (Non-Cloud)	CMS ARS v. 3.1 Cloud Baseline	MARS-E v. 2.2
DM-3	Minimization of PII Used in Testing, Training, and Research			DM-3 (1)		DM-3 (1)	DM-3 (1)	DM-3 (1)
IP-1	Consent			IP-1 (1)		IP-1 (1)	IP-1 (1)	IP-1 (1)
IP-2	Individual Access			IP-2		IP-2	IP-2	IP-2
IP-3	Redress			IP-3		IP-3	IP-3	IP-3
IP-4	Complaint Management			IP-4 (1)		IP-4 (1)	IP-4 (1)	IP-4 (1)
SE-1	Inventory of Personally Identifiable Information			SE-1		SE-1	SE-1	SE-1
SE-2	Privacy Incident Response			SE-2		SE-2	SE-2	SE-2
TR-1	Privacy Notice			TR-1 (1)		TR-1 (1)	TR-1 (1)	TR-1 (1)
TR-2	System of Records Notices and Privacy Act Statements					TR-2(1)	TR-2 (1)	
TR-3	Dissemination of Privacy Program Information			TR-3		TR-3	TR-3	TR-3
UL-1	Internal Use			UL-1		UL-1	UL-1	UL-1
UL-2	Information Sharing with Third Parties			UL-2		UL-2	UL-2	UL-2

Appendix C. Controls with Cloud Implications

A cloud environment requires, as shown in Table 20, implementation of specific security and privacy controls. In addition, there are certain requirements for cloud systems are also good practices that are strongly recommended in non-cloud environments as shown in Table 21. Table 22 presents other controls that are required for both environments but that have special tailoring for cloud environments. Every security and privacy control that has cloud implications in the SSP in Volume 2 will indicate the cloud designation in the control title.

Table 21. Controls Required for Cloud Environment Only

Control No.	Security / Privacy Control Name
AC-2(5)	Inactivity Logout
AC-2(12)	Account Monitoring / Atypical Usage
CM-5(1)	Automated Access Enforcement / Auditing
CM-5(3)	Signed Components
CM-10(1)	Open Source Software
SC-6	Resource Availability

Table 22. Controls Required for Cloud Environment and Recommended for Non-Cloud Environments

Control No.	Security / Privacy Control Name
AC-2(9)	Restrictions on Use of Shared Groups / Accounts
AC-2(10)	Shared / Group Account Credential Termination
AU-9(2)	Audit Backup on Separate Physical Systems / Components
CM-2(2)	Automation Support for Accuracy/Currency
CP-9(3)	Separate Storage for Critical Information
IA-2(11)	Remote Access – Separate Device
IA-4 (4)	Identify User Status
IA-5(6)	Protection of Authenticators
IR-9(1)	Responsible Personnel
IR-9(3)	Post-Spill Operations
RA-5(6)	Automated Trend Analyses
RA-5(8)	Review Historic Audit Logs
SA-10(1)	Software / Firmware Integrity Verification
SA-11(8)	Dynamic Code Analysis
SI-3(7)	Nonsignature-based Detection

Table 23. Controls with Special Tailoring for the Cloud Environment

Control No.	Security / Privacy Control Name
AC-8	System Use Notification
AU-2	Audit Events
AU-3(1)	Additional Audit Information
AU-6	Audit Review, Analysis, and Reporting
AU-8(1)	Synchronization with Authoritative Time Source
CM-8	Information System Component Inventory
CM-8(3)	Automated Unauthorized Component Detection
CP-7	Alternate Processing Site
CP-9	Information System Backup
IA-5(1)	Password-Based Authentication
IR-3	Incident Response Testing
MP-6	Media Sanitization
PE-14	Temperature and Humidity Controls
PS-5	Personnel Transfer
SC-28	Protection of Information at Rest
SC-28(1)	Cryptographic Protection

Appendix D. Crosswalk to 45 CFR §155.260

Table 24. Mapping of 45 CFR §155.260 to MARS-E Version 2.2 Security and Privacy Controls[3]

§155.260 Requirement	MARS-E v. 2.2 Security Controls	MARS-E v. 2.2 Privacy Controls
Creation, collection, use and disclosure "…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 IP-1: Consent

[3] 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 v. 2.2 Security Controls	MARS-E v. 2.2 Privacy Controls
(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 IP-1: Consent
(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 and that the uses and disclosures are also permissible under relevant law and policy.	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 AP-1: Authority to Collect AR-8: Accounting of Disclosures
(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.		

§155.260 Requirement	MARS-E v. 2.2 Security Controls	MARS-E v. 2.2 Privacy Controls
(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	AP-1: Authority to Collect 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; 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 and that the uses and disclosures are also permissible under relevant law and policy.	* Privacy issue	IP-2: Individual Access TR-3: Dissemination of Privacy Program Information

§155.260 Requirement	MARS-E v. 2.2 Security Controls	MARS-E v. 2.2 Privacy Controls
(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	AP-1: Authority to Collect 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 v. 2.2 Security Controls	MARS-E v. 2.2 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

§155.260 Requirement	MARS-E v. 2.2 Security Controls	MARS-E v. 2.2 Privacy Controls
(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
(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	AP-2: Purpose Specification DM-1: Minimization of Personally Identifiable Information DM-1 (1): Locate / Remove / Redact / Anonymize PII UL-1: Internal Use

§155.260 Requirement	MARS-E v. 2.2 Security Controls	MARS-E v. 2.2 Privacy Controls
(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 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	AR-2: Privacy Impact and Risk Assessment AR-4: Privacy Monitoring and Auditing DM-1: Minimization of Personally Identifiable Information SE-1: Inventory of Personally Identifiable Information [partial match] SE-2: Privacy Incident Response

§155.260 Requirement	MARS-E v. 2.2 Security Controls	MARS-E v. 2.2 Privacy Controls
(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-11: Audit Record Retention AU-12: Audit Generation CA-7: Continuous Monitoring All IR Controls RA-3: Risk Assessment RA-5: Vulnerability Scanning	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
(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 AR-4: Privacy Monitoring and Auditing AR-7: Privacy-Enhanced System Design and Development DM-1: Minimization of Personally Identifiable Information DM-1 (1): Locate / Remove / Redact / Anonymize PII

§155.260 Requirement	MARS-E v. 2.2 Security Controls	MARS-E v. 2.2 Privacy Controls
(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 AR-4: Privacy Monitoring and Auditing 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 v. 2.2 Security Controls	MARS-E v. 2.2 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 PL-2: System Security Plan 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 v. 2.2 Security Controls	MARS-E v. 2.2 Privacy Controls
(**b) Application to Non-Exchange Entities.** (b) (1) Non-Exchange Entities. A Non-Exchange Entity is any individual or entity that: Gains access to personally identifiable information submitted to an Exchange; or 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-3: System Development Life Cycle SA-4: Acquisition Process	AR-1: Governance and Privacy Program AR-3: Privacy Requirements for Contractors and Service Providers AR-7:Privacy-Enhanced System Design and Development
(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

§155.260 Requirement	MARS-E v. 2.2 Security Controls	MARS-E v. 2.2 Privacy Controls
(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
(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.	CA-3: System Interconnections 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
(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

§155.260 Requirement	MARS-E v. 2.2 Security Controls	MARS-E v. 2.2 Privacy Controls
(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 MP-1: Media Protection Policy and Procedures PE-1: Physical and Environmental Protection Policy and Procedures PL-1: Security Planning Policy and ProceduresPS-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	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 v. 2.2 Security Controls	MARS-E v. 2.2 Privacy Controls
(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.”	All “-1” Security Controls AT-2: Security Awareness Training AT-3: Role-Based Security Training PL-4: Rules of Behavior 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]
“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.”	All “-1” Security Controls 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
“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

§155.260 Requirement	MARS-E v. 2.2 Security Controls	MARS-E v. 2.2 Privacy Controls
(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]
(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 Also see IRS Publication 1075 (*Tax Information Security Guidelines for Federal, State, and Local agencies*)	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

Term	Definition
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
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

Term	Definition
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
FFE	Federally-Facilitated Exchange
FIPPS	Fair Information Protection Principles
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
FOIA	Freedom of Information Act
FTI	Federal Tax Information
FTP	File Transfer Protocol
GAGAS	Generally Accepted Governmental Auditing Standards
GMT	Greenwich Meridian Time
HHS	Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act of 1996

Term	Definition
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

Term	Definition
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

Term	Definition
SBE	State-Based Exchange
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

Term	Definition
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
zONE	Opportunity to Network and Exchange

Master Glossary for MARS-E Document Suite

Term

Definition

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 Exchange 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 Exchange.

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.

Term	Definition
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.
Exchange	American Health Exchange established under Sections 1311(b), 1311(d), or 1321(c) (1) of the ACA, including both State-Based Exchanges (SBEs) and Federally-Facilitated Exchanges (FFE). The use of the term "Exchange" in this Framework indicates that a control applies to both SBEs and FFEs.

Term **Definition**

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. Exchange privacy and security regulations at 45 CFR §155.260(a) (3) (i)-(viii) require that Exchanges 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 Exchange (FFE)

An Exchange 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.

Term	Definition
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 Exchange, 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	Incident means an occurrence that actually or imminently jeopardizes, without lawful authority, the confidentiality, integrity, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies (44 U.S.C. § 3552).
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.

Term	Definition
Insurance Affordability Program	Program under Title I of the ACA for the enrollment in qualified health plans offered through an Exchange, 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.
Medicaid	The Medicaid program was established under Title XIX of the Social Security Act, together with other health care programs established under state law.

Term **Definition**

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 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)

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 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. […]"

Personally Identifiable Information (PII)

As defined by OMB Memorandum M-17-12 (January 3, 2017), the term PII refers to 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 Exchange 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.

Term	Definition
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 Exchange, 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 Exchange in which it is sold.
Qualified Individual	With respect to an Exchange, an individual who has been determined eligible to enroll through the Exchange 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.
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 Exchange (SBE)	As authorized by the Affordable Care Act, a health insurance Exchange 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 Exchange.

Term **Definition**

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://zone.cms.gov/document/annual-security-and-privacy-attestation-procedure-aca-systems

2. Security and Privacy Oversight and Monitoring Guide for Administering Entity (AE) Systems in Operation, available at: https://zone.cms.gov/document/security-and-privacy-oversight-and-monitoring-guide-ae-systems-operation

3. Change Reporting Procedures for State-Based Administering Entity Systems, available at: https://zone.cms.gov/document/change-reporting-procedures-administering-entities-aca-systems

4. Framework for Independent Assessment of Security and Privacy Controls, available at: https://zone.cms.gov/document/framework-independent-assessment-security-and-privacy-controls

5. State-based Exchange (SBM) IT Decommissioning and Data Retention Planning, available at: https://zone.cms.gov/document/decommissioning-and-data-retention-planning

6. Administering Entity Security and Privacy Incident Report template , available at: https://zone.cms.gov/document/aca-administering-entity-ae-incident-response-ir

7. Fed2NonFed Interconnection Security Agreement template, available at: https://zone.cms.gov//document/fed2nonfed-interconnection-security-agreement-isa

8. State Plan of Action and Milestones, Template, available at: https://zone.cms.gov/document/plan-action-and-milestones-template

9. Information Security Risk Assessment (ISRA) Template Instructions, available at: https://zone.cms.gov/document/information-security-risk-assessment-isra-procedure

10. Affordable Care Act Health Insurance Administering Entity Privacy Impact Assessment (PIA) template and guide, available at: https://zone.cms.gov/document/privacy-impact-assessment-pia

11. Information Exchange Agreement Template, available at: https://zone.cms.gov//document/information-exchange-agreement-iea

12. Computer Matching Agreement (CMA) between CMS and State-Based Administering Entities, available at: https://zone.cms.gov/document/computer-matching-agreement; Electronic Authentication Guidelines for ACA Administering Entity Systems, available at: https://zone.cms.gov/document/e-authentication-guidelines-aca-administering-entities-aes

13. CMS Security and Privacy MARS-E Timelines and Artifacts List: https://zone.cms.gov/document/cms-security-and-privacy-mars-e-timelines-and-artifacts-list

14. CMS Acceptable Risk Safeguards (ARS): https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/ARS-31-Publication

Federal Legislation, Guidance, and Regulations

1. Public Law 111–148, Patient Protection and Affordable Care Act, March 23, 2010, 124 Stat. 119, available at: https://www.congress.gov/111/plaws/publ148/PLAW-111publ148.pdf

2. Public Law 74-271, Social Security Act, as amended, available at: http://www.ssa.gov/OP_Home/ssact/ssact.htm

3. 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.archives.gov/about/laws/privacy-act-1974.htmlPublic Law 104-13, Paperwork Reduction Act of 1995, as amended, available at: http://www.fws.gov/policy/library/rgpl104-13.pdf

4. Code of Federal Regulations (CFR), Regulation 5 CFR Part 731 – Suitability, 5CFR731, available at: https://www.govinfo.gov/app/details/CFR-2012-title5-vol2/CFR-2012-title5-vol2-sec731-202

5. United States Code Title 44, Chapter 33—Disposal of Records, available at: http://www.archives.gov/about/laws/disposal-of-records.html

6. *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

7. Office of Management and Budget (OMB), Memorandum M-07-16, *Safeguarding and Responding to the Breach of Personally Identifiable Information,* May 22, 2007, available at https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2007/m07-16.pdf

8. 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: https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final

9. NIST SP 800-53A Rev 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans,* December 2014, available at: https://csrc.nist.gov/publications/detail/sp/800-53a/rev-4/final

10. NIST SP 800-63-3, *Digital Identity Guidelines* 03-02-2020, available at https://csrc.nist.gov/publications/detail/sp/800-63/3/final

11. NIST SP 800-66 Rev 1, *An Introductory Resource Guide for Implementing the HIPAA Security Rule,* October 2008, available at: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-66r1.pdf

12. NIST SP 800-145, *The NIST Definition of Cloud Computing*, September 2011, available at: https://csrc.nist.gov/publications/detail/sp/800-145/final

13. NIST SP 800-88 Revision 1, *Guidelines for Media Sanitization*, December 2014, available at: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf

14. Federal Information Processing Standards (FIPS) Publication (PUB) 199, *Standards for Security Categorization of Federal Information and Information Systems,* NIST, February 2004, available at: https://csrc.nist.gov/csrc/media/publications/fips/199/final/documents/fips-pub-199-final.pdf

15. FIPS Publication (PUB) 200, *Minimum Security Requirements for Federal Information and Information Systems*, NIST, May 2006, available at: http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf

16. 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

17. *e-Government Act of 2002*. https://www.congress.gov/107/plaws/publ347/PLAW-107publ347.pdf

18. Federal Information Security Management Act of 2002, available at: http://csrc.nist.gov/groups/SMA/fisma/index.html

19. Health Insurance Portability and Accountability Act of 1996, available at: http://www.gpo.gov/fdsys/pkg/PLAW-104publ191/content-detail.html

20. Privacy Act of 1974, available at: https://www.cms.gov/PrivacyActof1974/

21. Patient Protection and Affordable Care Act, Public Law 111–148, March 23, 2010, 124 Stat. 119, available at: https://www.congress.gov/111/plaws/publ148/PLAW-111publ148.pdf Amendment(s) to 45 CFR Part 155.260 published March 11, 2014, in 79 FR 13837 https://www.govregs.com/regulations/expand/title45_chapterA_part155_subpartC_section155.260 Department of Health and Human Services Regulations

22. 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: https://www.ecfr.gov/cgi-bin/text-idx?SID=538dba54a78a1694d7e227e9d8fb4be0&mc=true&node=pt45.1.155&rgn=div5