Centers for Medicare & Medicaid Services

Minimum Acceptable Risk Standards for Exchanges – Exchange Reference Architecture Supplement

Version 1.0

August 1, 2012

Executive Overview

The Patient Protection and Affordable Care Act of 2010[1] (hereafter simply the "Affordable Care Act") provides for each state to have a health insurance Exchange. An Exchange is an organized marketplace to help consumers and small businesses buy health insurance in a way that permits easy comparison of available plan options based on price, benefits and services, and quality. Consumers seeking health care coverage will be able to go to the health insurance Exchanges to obtain comprehensive information on coverage options currently available and make informed health insurance choices. By pooling consumers, reducing transaction costs, and increasing transparency, Exchanges create more efficient and competitive health insurance markets for individuals and small businesses.

Section 1561 of the Affordable Care Act requires the Department of Health and Human Services (HHS), in consultation with the Health Information Technology (HIT) Policy Committee and the HIT Standards Committee (the Committees), to develop interoperable and secure standards and protocols that facilitate electronic enrollment of individuals in federal and state health and human services programs.

In order to ensure the use of these Exchanges and common program enrollment systems, public trust is essential and must be established by adoption of strong security and privacy protections for these information technology (IT) systems. Studies consistently show that while consumers have a favorable view of new healthcare technology and are willing to share their own Personally Identifiable Information (PII), Protected Health Information (PHI), or financial information, they remain concerned about the adequacy of security and privacy protection of this information.

Federal statutes and regulations require the U.S. Government to protect its IT systems and the information contained within those systems, ensuring the application of reasonable IT security and privacy controls for those parties with whom the federal government shares information. At present, there is a complex array of regulations and requirements that govern federal and state protection of IT security and privacy.

The establishment of health insurance Exchanges and common program enrollment systems must address certain federal legislation and regulations. The most significant federal laws and regulations for consideration are:

- **Federal Information Security Management Act (FISMA)**, which controls the development, documentation, and implementation of programs to provide security for information and information systems
- **Health Insurance Portability and Accountability Act of 1996 (HIPAA)**, which establishes national standards for electronic healthcare transactions and national identifiers for providers, health insurance plans, and employers, and sets forth privacy and security standards for handling health information

[1] Public Law 111–148, Patient Protection and Affordable Care Act, March 23, 2010, 124 Stat. 119, http://www.gpo.gov/fdsys/pkg/PLAW-111publ148/content-detail.html
http://www.healthreform.gov/health_reform_and_hhs.html

- **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, which establishes privacy and security controls required for processing Exchange applicant information
- **Internal Revenue Code (IRC), 26 U.S.C. §6103**, which establishes criteria for handling Federal Tax Information (FTI)

In addition, numerous other federal and state regulations impact the processes for securing information. For example, the Privacy Act of 1974 places limitations on the collection, disclosure, and use of certain personal information, including PHI. The e-Government Act of 2002 requires federal agencies to conduct privacy impact assessments (PIA) associated with collecting, maintaining, and disseminating PII. The Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH) promotes the adoption and meaningful use of HIT. State statutes, such as the California Senate Bill CSB 1381, protect in varying degrees the privacy of PII and PHI.

There is no integrated, comprehensive approach to security and privacy that respects applicable federal requirements under FISMA, HIPAA, HITECH, ACA, the Privacy Act, Tax Information Safeguarding Requirements, and state and other federal regulations. Therefore, to facilitate compliance with the myriad of security requirements for Exchange and common program enrollment systems, CMS developed this *Minimum Acceptable Risk Standards for Exchanges – Exchange Reference Architecture Supplement* (hereafter simply “MARS-E”).

Protecting and ensuring the confidentiality, integrity, and availability for Exchange and common program enrollment information and information systems is the responsibility of the Exchanges. The Affordable Care Act charges CMS with responsibility for oversight of the Exchange and common enrollment IT systems. Since the Exchanges and the federal government must share data and otherwise integrate IT systems for the implementation and operation of the health insurance Exchanges and common program enrollment, this document defines a set of minimum set of standards for acceptable security risk that the Exchanges must address.

This document provides an explanation of the Minimum Security Controls for Exchanges structure, including Minimum Security Controls Family Numbering and Description, Control Requirements, and Assessment Procedures. A companion document, the *Catalog of Minimum Acceptable Risk Controls for Exchanges – Exchange Reference Architecture Supplement*, presents the specific controls and details.

The laws and guidance provided by other federal agencies and the National Institute for Standards and Technology remain the authoritative source. Depending on the information processed, an Exchange’s IT system may be required to meet additional security control requirements as mandated by specific federal, state, legal, program, or accounting sources. For example, when Exchanges handle PHI, they are subject to HIPAA regulations and standards. In addition, IRC §6103 applies if an Exchange IT system receives FTI. Therefore, Exchanges must develop their IT systems to comply with these more stringent standards[2] when applicable. The

[2] For example, National Institute of Standards and Technology Special Publication 800-66, Revision 1, *An Introductory Resource Guide for Implementing the HIPAA Security Rule*, discusses security considerations and resources for use when implementing the requirements of the Security Rule. For FTI, Exchange IT system owners should follow IRS Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies.

guidance in the *MARS-E* neither relieves nor waives any other federal, state, or other applicable laws, guidance, policies, or standards.

Foreword

The *Exchange Reference Architecture: Foundation Guidance,* Version 1.0, provides the business, information, and technical architecture approach and technical standards for the health insurance Exchanges. The Foundation Document provides an overview and description of the approaches to defining the architectures; the Centers for Medicare & Medicaid Services (CMS) will release additional Exchange Reference Architecture (ERA) supplements to provide engineering detail allowing Exchange implementation and operations personnel to build systems and environments that adhere to the approved Exchange architecture as well as other state information technology (IT) standards, data safeguards, and requirements.

CMS's Deputy Chief Information Officer (DCIO) leads the development of this Architecture with the support of the Exchanges and all components of the IT staff and contractors. The ERA consists of the Foundation Guidance document and the CMS ERA Supplements, authorized and approved by the CMS DCIO. CMS has reviewed and accepted this Architecture Framework as a foundational component of CMS's Enterprise Architecture in accordance with the CMS IT governance process.

In accordance with the agency's Information Security program, CMS has developed two companion documents, the *Catalog of Minimum Acceptable Risk Controls for Exchanges – Exchange Reference Architecture Supplement* and the *Harmonized Security and Privacy Framework – Exchange Reference Architecture Supplement.* Together, these documents, along with the four documents in the Affordable Care Act (ACA) System Security Plan Document Suite,[3] form Version 1.0 of the *Minimum Acceptable Risk Standards for Exchanges* Document Suite (also known as the "MARS-E Suite").

The guidance contained in these documents also applies to other Affordable Care Act Administering Entities. "Administering Entity" means a state Medicaid Agency, state Children's Health Insurance Program (CHIP), a state basic health program (BHP), or an Exchange.

This *Minimum Acceptable Risk Standards for Exchanges – Exchange Reference Architecture Supplement* and the *Harmonized Security and Privacy Framework – Exchange Reference Architecture Supplement* (see Reference 2, List of References) define a risk-based Security and Privacy Framework for use in the design and implementation of Exchange IT systems for which CMS has oversight responsibility. CMS has reviewed and accepted the *Minimum Acceptable Risk Standards for Exchanges* as a component of the Exchange Reference Architecture in accordance with the CMS IT governance process.

Any changes to this *Minimum Acceptable Risk Standards for Exchanges – Exchange Reference Architecture Supplement* must be approved by the CMS DCIO, the CMS Chief Information Security Officer, and the CMS Chief Technology Officer.

[3] The suite consists of the *ACA System Security Plan Procedures*, Version 1.0; *ACA System Security Plan Template*, Version 1.0; *ACA System Security Plan*, Attachment 1 SSP Workbook; and *ACA System Security Plan, Attachment 2 Safeguard Procedures Report Template*.

Error! No text of specified style in document.

Tony Trenkle Date
Chief Information Officer
Centers for Medicare & Medicaid Services

Henry Chao Date
Deputy Chief Information Officer
Centers for Medicare & Medicaid Services

Mark Hogle Date
Chief Technology Officer
Centers for Medicare & Medicaid Services

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

Federal Partner Agency Concurrence and Approval

The following federal partner agency signatories have reviewed and concur with the guidance contained in the following documents known as the MARS-E Document Suite:

- *Harmonized Security and Privacy Framework – Exchange Reference Architecture Supplement*, Version 1.0
- *Minimum Acceptable Risk Standards for Exchanges – Exchange Reference Architecture Supplement*, Version 1.0
- *Catalog of Minimum Acceptable Risk Controls for Exchanges – Exchange Reference Architecture Supplement*, Version 1.0
- *ACA System Security Plan Procedures*, Version 1.0
- *ACA System Security Plan Template*, Version 1.0
- *ACA System Security Plan, Attachment 1 SSP Workbook*
- *ACA System Security Plan, Attachment 2 Safeguard Procedures Report Template*

SEEN AND APPROVED:

Internal Revenue Service

Terence V. Milholland ______________/s/______________ ____________
Chief Technology Officer Signature Date

S. Gina Garza ______________/s/______________ ____________
ACIO, Affordable Care Act (PMO) Signature Date

Social Security Administration

Kelly Croft ______________/s/______________ ____________
Deputy Commissioner for Systems and Chief Information Officer Signature Date

Brad Flick ______________/s/______________ ____________
Associate Commissioner and Chief Information Security Signature Date

Department of Veterans Affairs

Jerry Davis ______________/s/______________ ____________
Deputy Assistant Secretary and Chief Information Security Officer Signature Date

John Oswalt ______________/s/______________ ____________
Associate Deputy Assistant Secretary for Policy, Privacy and Incident Response Signature Date

Department of Homeland Security

Mark Schwartz /s/
USCIS Chief Information Officer Signature Date

Perry Darley /s/
USCIS Chief Information Security Signature Date
Officer

Department of Defense

Dr. Karen Guice /s/
Chief Information Officer Signature Date

COL Lorraine Breen /s/
Acting Chief Information Officer Signature Date

Peace Corps

Dorine Andrews /s/
Chief Information Officer Signature Date

Falan Memmott /s/
Director of IT Security Assurance Signature Date
& Compliance

Office of Personnel Management

Matthew Perry /s/
Chief Information Officer Signature Date

Andy Newton /s/
Chief Information Security Officer Signature Date

Record of Changes

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

CR: Change Request

Table of Contents

List of Tables

1. Introduction

The Patient Protection and Affordable Care Act of 2010[4] (hereafter simply the "Affordable Care Act") provides for each state to have a health insurance Exchange. An Exchange is an organized marketplace to help consumers and small businesses buy health insurance in a way that permits easy comparison of available plan options based on price, benefits and services, and quality. Consumers seeking health care coverage will be able to go to the health insurance Exchanges to obtain comprehensive information on coverage options currently available and make informed health insurance choices. By pooling consumers, reducing transaction costs, and increasing transparency, Exchanges create more efficient and competitive health insurance markets for individuals and small employers.

One of the key ACA implementation considerations is the protection of the confidentiality of applicant information, as stated in Section 1411(g) of the Affordable Care Act. Furthermore, Section 1561 of the Affordable Care Act requires the Department of Health and Human Services (HHS), in consultation with the Health Information Technology (HIT) Policy Committee and the HIT Standards Committee (the Committees), to develop interoperable and secure standards and protocols that facilitate electronic enrollment of individuals in federal and state health and human services programs.

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

The Department's Final Rule on the implementation of ACA Exchanges, released on March 12, 2012, provides conditions for the creation, collection, use, and disclosure of Personally Identifiable Information (PII) for the purpose of determining eligibility for enrollment in a qualified health plan.

1.1 Background

Adoption of strong security and privacy protections is necessary to ensuring the public trust. Studies consistently show that while consumers have a favorable view of new healthcare technology and are willing to share their own PII, Protected Health Information (PHI), or Federal Tax Information (FTI), they remain concerned about the adequacy of security and privacy protection of this information.

CMS published the *Harmonized Security and Privacy Framework – Exchange Reference Architecture Supplement* (see Reference 2, *List of References)* to provide guidance on security and privacy considerations essential to establishing a Harmonized Security and Privacy Framework for the Exchange Reference Architecture. The Harmonized Security and Privacy Framework addresses the following security and privacy topics at the conceptual level:

[4] Public Law 111–148, Patient Protection and Affordable Care Act, March 23, 2010, 124 Stat. 119, http://www.gpo.gov/fdsys/pkg/PLAW-111publ148/content-detail.html http://www.healthreform.gov/health_reform_and_hhs.html

- System and Data Classification
- Security Controls
- Identity, Credential, and Access Management
- Secure Infrastructure and Cloud Computing
- Data Encryption
- Audit Trails
- Continuity of Operations and Disaster Recovery
- Compliance Oversight
- Privacy

Protecting and ensuring the confidentiality, integrity, and availability of information systems and associated data is the responsibility of the Exchanges; the Affordable Care Act charges CMS with responsibility for oversight of the Exchange and common enrollment IT systems. Since the Exchanges and the federal government must share data and otherwise integrate IT systems for the implementation and operation of the health insurance Exchanges, this document defines a set of minimum set of security requirements that the Exchanges must address.

1.1.1 Approach

Given the constraints in resources and implementation schedule, CMS initially took a minimalist approach to identify a critical set of security controls deemed essential to address the most prevalent threats. The guidance provided in earlier versions of this ERA Supplement reflects industry and government best practices to support a viable, effective approach that address Consensus Audit Guidelines (CAG) Top 20 critical security controls as published by SANS[5]. However, as the result of IRS review and request from exchanges asking for a minimum set that includes IRS FTI Safeguards requirements, the Catalog of Minimum Security Controls for Exchanges has been expanded to include FTI protection requirements.

1.2 Purpose

Section 155.260 (a)(3) of the HHS Final Rule on ACA Exchanges requires each Exchange to establish and implement privacy and security standards consistent with the principles stated in §155.260 of the Rule. The purpose of this *MARS-E* is to provide a starting point for security guidance that Exchanges can use in implementing and operating their IT systems in support of the Affordable Care Act. Each Exchange system owner is responsible for incorporating the security controls defined in this document with other state-appropriate security and privacy requirements for protecting PII against anticipated threats or unlawful use.

Depending on the information processed, an Exchange’s IT system may be required to meet additional security control requirements as mandated by specific federal, state, legal, program, or accounting sources. For example, depending on the data being processed, an Exchange may be a “covered entity” under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act of 2009

[5] See http://www.sans.org/critical-security-controls/

(HITECH). When Exchanges handle PHI, they are subject to these laws. In addition, Internal Revenue Code (IRC) 26 U.S.C. §6103 applies if an Exchange IT system receives Federal Tax Information. Therefore, Exchanges must develop their IT systems to comply with these more stringent standards[6] when applicable. Exchanges must document such requirements and the control implementation details in their System Security Plans (SSP). Exchanges also are required to define system risks in an Information Security (IS) Risk Assessment (RA). The guidance in the *MARS-E* neither relieves nor waives any other federal, state, or other applicable laws, guidance, policies, or standards.

1.3 Scope

This document focuses on Exchange IT systems. The minimum security controls identified by this supplement assume that the applicable IT system is classified as Moderate[7] and contains PII.

1.4 Related Documents

The List of References presents additional guidance and sources used in preparing the *MARS-E.* CMS established and separately maintains the companion *Catalog of Minimum Acceptable Risk Controls for Exchanges – Exchange Reference Architecture Supplement*, which presents the specific control requirements for each Exchange IT system for which CMS has oversight responsibility*.*

Other related documents include those developed for the CMS Information Security program that comply with federal mandates and CMS requirements for the handling and processing of CMS's information and information systems.[8]

1.5 Intended Audience

The *Minimum Acceptable Risk Standards for Exchanges – Exchange Reference Architecture Supplement* provides guidance to Exchanges and their contractors regarding the minimum level security controls that must be implemented to protect information and information systems for which CMS has oversight responsibility, and has received the explicit approval of the CMS Deputy Chief Information Officer (DCIO) and the CMS Chief Information Security Officer (CISO). CMS has authorized distribution of this document to all Exchanges, other federal agencies, CMS staff, CMS Production Environment contractors, The MITRE Corporation [the agency's Federally Funded Research and Development Center (FFRDC) advisor], and any entity given explicit access to this document through CMS executive or management approval.

[6] For example, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-66, Revision 1, *An Introductory Resource Guide for Implementing the HIPAA Security Rule*, discusses security considerations and resources for use when implementing the requirements of the Security Rule. For FTI, Exchange IT system owners should follow IRS Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies.

[7] See NIST Federal Information Processing Standards (FIPS) Publication (Pub) 199, *Standards for Security Categorization of Federal Information and Information Systems.*

[8] The CMS IS web site at http://www.cms.gov/InformationSecurity/ISD/list.asp?listpage=1 provides a list of applicable laws across the program. The CMS IS web site at http://www.cms.hhs.gov/InformationSecurity/ provides a list of applicable CMS documents across the IS program.

1.6 Document Organization

This document is organized as follows:

Section	Purpose
Section 2: Security Guidance	Provides a high-level explanation of security guidance presented in the *Minimum Acceptable Risk Standards for Exchanges.*
Section 3: Minimum Security Controls for Exchanges Structure	Provides a high-level explanation of the Minimum Security Controls for Exchanges structure, including Minimum Security Controls Family Numbering and Description, Control Requirements, and Assessment Procedures.
Acronyms	Defines the acronyms used in this document.
List of References	Lists the sources used in preparing this document.

2. Security Guidance

The *MARS-E* establishes minimum security control guidance for all Exchange IT information systems for which CMS has oversight responsibility, starting with Exchanges and common program enrollment systems as required by the Affordable Care Act. All Exchange employees, contractors, subcontractors, and their respective facilities supporting such IT systems shall observe the controls defined in the *MARS-E* and in the *Catalog of Minimum Acceptable Risk Controls for Exchanges – Exchange Reference Architecture Supplement.* Section §155.260 of the HHS Final Rule stipulates that Exchanges must require the same or more stringent privacy and security standards as a condition of contract or agreement with individuals or entities, such as Navigators, agents, and brokers that have access to Exchange-owned PII.

An Exchange system owner may choose to strengthen the controls implementation beyond the defined requirements to provide additional protection of Exchange IT information and information systems. In some cases, the system owner may implement the control on a parent system and have subordinate systems inherit the control from the parent system.

This *MARS-E* covers the implementation of the critical technical, management, and operational controls needed to defend against the most common and damaging computer and/or network attacks. The critical controls are:

- Inventory of authorized and unauthorized devices
- Inventory of authorized and unauthorized software
- Secure configurations for hardware and software
- Secure configurations of such network devices such as firewalls, routers, and switches
- Boundary defense
- Maintenance, monitoring, and analysis of security audit logs
- Application software security
- Controlled use of administrative privileges
- Controlled access based on need-to-know
- Continuous vulnerability assessment and remediation
- Account monitoring and control
- Malware defenses
- Limitation and control of network ports, protocols, and services
- Wireless device control
- Data loss prevention
- Secure network engineering
- Penetration tests and red team exercises
- Incident response capability
- Data recovery capability
- Security skills assessment and training to fill gaps

Identify data elements sourced from federal agencies

3. Minimum Security Controls for Exchanges Structure

The structure of the Minimum Security Controls for Exchanges employs NIST SP 800-53, Rev 3, *Recommended Security Controls for Federal Information Systems and Organizations* family numbering, descriptions and control requirements; NIST SP 800-53 A, Rev 1*, Guide for Assessing the Security Controls in Federal Information Systems and Organizations* provides the assessment procedures. The following subsections present a description of the Family Numbering, Controls Structure, and Assessment Procedures. For the most part, these subsections comprise an abbreviated discussion of content found in the two NIST documents.

3.1 Minimum Security Controls for Exchanges Family Numbering and Description

CMS has organized the Minimum Security Controls into control families within three classes: management, operational, and technical. The *Catalog of Minimum Acceptable Risk Controls for Exchanges – Exchange Reference Architecture Supplement* presents the security controls. Each family contains security controls related to the security functionality of the family. A two-character identifier, Family ID, is assigned to uniquely identify each of the security control families. Fourteen of the NIST SP 800-53 control families were selected for the *Catalog of Minimum Acceptable Risk Controls for Exchanges – Exchange Reference Architecture Supplement*. Table 1 summarizes and the control families and identifies the two-character identifier associated with each family.

Table 1. Family Descriptions for Minimum Security Controls for Exchanges

Family (and Identifier)	Class	Description
Access Control (AC)	Technical	The standards listed in this section focus on how the Exchange shall limit IT system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems), and to the types of transactions and functions that authorized users are permitted to exercise.
Awareness and Training (AT)	Operational	The standards listed in this section focus on how the Exchange shall: (i) ensure that managers and users of Exchange IT systems are made aware of the security risks associated with their activities and of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures related to the security of IT systems; and (ii) ensure that Exchange personnel are adequately trained to carry out their assigned IS-related duties and responsibilities.
Audit and Accountability (AU)	Technical	The standards listed in this section focus on how the Exchange shall: (i) create, protect, and retain IT system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate IT system activity; and (ii) ensure that the actions of individual IT system users can be uniquely traced to those users so they can be held accountable for their actions.

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

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

Family (and Identifier)	Class	Description
System and Information Integrity (SI)	Operational	The standards listed in this section focus on how the Exchange shall: (i) identify, report, and correct information and IT system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within Exchange IT systems; and (iii) monitor IT system security alerts and advisories, and take appropriate actions in response.
Program Management (PM)	Management	The standards listed in this section complement the security controls in the above 17 families by focusing on the organization-wide information security requirements that are essential for managing information security programs.
FTI Safeguards		The standards listed in this section are additional controls required by IRS Publication 1075

3.2 Control Structure

The Minimum Security Controls for Exchanges structure consists of seven sections: Baseline and Implementation Standards, Enhancement Control, Guidance, Applicability, Reference, Related Control Requirements, and Assessment Procedure. The following subsections provide a brief description of the structure of each section of the controls.

3.2.1 Baseline Control

The Baseline control is the concise statement specifying the capability needed to protect a particular aspect of the Exchange IT system for which CMS has oversight responsibility, starting with those Exchange systems that support the Affordable Care Act.

Security control Family ID identifies the Baseline controls that convey recommended security policy statements based on NIST SP 800-53.

3.2.1.1 Implementation Standard

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

For example, CP-9’s second implementation standard states as follows:

> “(For PII only) Ensure that a current, retrievable, copy of PII is available before movement of servers.”

This particular implementation standard applies when Exchange IT systems store PII information.

Similar implementation standards exist and apply for Exchange for providing PHI data. In the absence of PHI or PII data—as evidenced by the statement “(For XXX only, XX meaning PHI or PII, for example)”—all other implementation standards are indicated and recommended.

Table 2 shows an example of the implementation standard associated with Minimum Security Control CP-9. Implementation standard item 1 is a recommended control that applies to all IT information and information systems. Item 2 is specifically designated for those organizations responsible for PII and must be followed for implementation, assessment, and audit.

Table 2. Implementation Standards for Minimum Security Control for Exchanges CP-9

Implementation Standard(s)
1. Perform full backups weekly to separate media. Perform incremental or differential backups daily to separate media. 2. (For PII only) Ensure that a current, retrievable copy of PII is available before movement of servers.

Table 3 provides definitions for PII, PHI, and FTI. Organizations responsible for these types of information must provide additional safeguards as defined in the implementation standards.

Table 3. Handling of Special Information

Term	Definition
Personally Identifiable Information	As defined by OMB (Memorandum M-07-16), 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.
Protected Health Information	Under HIPAA, the term "Protected Health Information" is individually identifiable health information that is held or transmitted in any form or medium by a covered entity.
Federal Tax Information	Generally, Federal tax returns and return information are confidential, as required by IRC §6103. The IRS uses this information to ensure that agencies, bodies, and commissions are maintaining appropriate safeguards to protect the information confidentiality.

3.2.2 Enhancement Control

Enhancement controls supplement baseline controls to achieve the overall required level of protection CMS deems necessary.

The Enhancement controls are structured the same as the Baseline controls with the exception of implementation standards. Each Enhancement section includes the following:

- Control Requirement
- Guidance (may not exist for all Enhancements)
- Assessment Procedure
  - Assessment Objectives
  - Assessment Methods and Objects

3.2.3 Guidance

The Baseline Controls may include a Guidance section to provide additional information on the intent of the control. In some cases, that guidance will include specific CMS preferences or recommendations, or may refer to other CMS or NIST publications for further guidance. Referring to other guidance and procedures for additional information is a good security practice to facilitate the organization's satisfaction of the required minimum security controls.

3.2.4 Applicability

An Exchange's IT system implementation and operation must meet all Minimum Security Controls for Exchanges.

3.2.5 Reference

The References section identifies the source documents and section or paragraph designations for which the specific control is also applicable. Implementing this control satisfies an element of a specific external requirement. For example, an IRS reference would appear as follows: IRS-1075: 9.2. From this example:

- The IRS-1075 is the publication.
- The 9.2 portion is the section with sub-paragraphs leading to the applicable reference used for the control requirement.

3.2.6 Related Control Requirements

Many, but not all, Minimum Security Controls for States may be related to one or more other Minimum Security Controls. These relationships may cause conflicts between controls. Therefore, when addressing some Minimum Security Controls for Exchanges in a security assessment or audit, organizations shall avoid, at the very least, conflicts between related responses and should ensure consistency in references to related Minimum Security Controls.

3.2.7 Assessment Procedures

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

3.2.7.1 Assessment Objectives

The Assessment Objectives include a set of determination statements ("Determine if…") related to the particular security control assessed. By closely linking the determination statements to the content of the security control (i.e., the security control functionality), the Exchange can ensure traceability of assessment results back to the fundamental control requirements. Each of the Assessment Objective determination statements is either traceable to requirements in the Baseline or Enhancement security control or the Guidance. This ensures that all aspects of the security control are assessed and that the organization can identify any weaknesses or deficiencies in the control and take remediation actions.

3.2.7.2 Assessment Methods and Objects

The Assessment Methods and Objects define the nature of the assessor's actions and the associated activity (i.e., Examine, Interview, and Test). The assessment object identifies the specific item assessed, including specifications, mechanisms, activities, and individuals. If the assessment procedure outcome is a determination that a security control was not implemented adequately, assessment findings are produced. These assessment findings subsequently help the Exchange determine the overall effectiveness of the control.

Acronyms

ACA	Patient Protection and Affordable Care Act of 2010
CAG	Consensus Audit Guidelines
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CMS	Centers for Medicare & Medicaid Services
CTO	Chief Technology Officer
DCIO	Deputy Chief Information Officer
ERA	Exchange Reference Architecture
FTI	Federal Tax Information
HHS	U.S. Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act of 1996
HITECH	Health Information Technology for Economic and Clinical Health Act of 2009
IRC	Internal Revenue Code
IRS	Internal Revenue Service
IS	Information Security
IS	Information System
MARS-E	Minimum Acceptable Risk Standards for Exchanges
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PHI	Protected Health Information
PII	Personally Identifiable Information
POA&M	Plan of Action & Milestones
RA	Risk Assessment
SP	Special Publication
SSP	System Security Plan

List of References

1. *Exchange Reference Architecture: Foundation Guidance,* Version 0.99, Centers for Medicare & Medicaid Services (CMS), March 16, 2011.
2. *Harmonized Security and Privacy Framework – Exchange Reference Architecture Supplement,* Draft, Version 0.99, CMS, March 16, 2012.
3. *Catalog of Minimum Acceptable Risk Controls for Exchanges – Exchange Reference Architecture Supplement, Draft,* Version 0.99, CMS, March 16, 2012.
4. Public Law 111–148, Patient Protection and Affordable Care Act, March 23, 2010, 124 Stat. 119, http://www.gpo.gov/fdsys/pkg/PLAW-111publ148/content-detail.html http://www.healthreform.gov/health_reform_and_hhs.html
5. Public Law 74-271, Social Security Act, as amended. http://www.ssa.gov/OP_Home/ssact/ssact.htm
6. Public Law 93-579, The Privacy Act of 1974, September 27, 1975, 88 Stat. 1896, 5 U.S.C. §552a, as amended.
7. Public Law 104-13, Paperwork Reduction Act of 1995, as amended. http://www.fws.gov/policy/library/rgpl104-13.pdf
8. Public Law 108–173, Medicare Prescription Drug, Improvement, and Modernization Act of 2003 (MMA), SEC. 912: Requirements for Information Security for Medicare Administrative Contractors. http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ173.108.pdf
9. Code of Federal Regulations (CFR), Regulation 5 CFR Part 731 – Suitability, 5CFR731. http://www.access.gpo.gov/nara/cfr/waisidx/5cfr731.html
10. United States Code Title 44, Chapter 33—Disposal of Records. http://www.archives.gov/about/laws/disposal-of-records.html
11. *Federal Information System Controls Audit Manual (FISCAM)*, Government Accountability Office, GAO-09-232G, February 2, 2009. http://www.gao.gov/new.items/d09232g.pdf
12. Office of Management and Budget (OMB), Memorandum M-07-16, *Safeguarding and Responding to the Breach of Personally Identifiable Information,* May 22, 2007.
13. Executive Orders can be found at: http://www.archives.gov/federal-register/executive-orders/disposition.html
14. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems*, August 2009.
15. NIST SP 800-53A, Revision 1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations,* June 2010.
16. NIST SP 800-63, Version 1.0.2, *Electronic Authentication Guidelines*, April 2006.
17. NIST SP 800-66, Revision 1, *An Introductory Resource Guide for Implementing the HIPAA Security Rule,* October 2008.

18. Federal Information Processing Standards (FIPS) Publication (PUB) 199, *Standards for Security Categorization of Federal Information and Information Systems,* NIST, February 2004.

19. FIPS Publication (PUB) 200, *Minimum Security Requirements for Federal Information and Information Systems*, NIST, March 2006.

20. 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

21. 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.