Extract for PE Control Family

540 Central

CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES

Centers for Medicare & Medicaid Services

Catalog of Minimum Acceptable Risk Controls for Exchanges – Exchange Reference Architecture Supplement

Version 1.0

August 1, 2012

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 Guidance 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 Exchange 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 this *Catalog of Minimum Acceptable Risk Controls for Exchanges – Exchange Reference Architecture Supplement* to establish the specific controls for data. Two companion documents, the *Harmonized Security and Privacy Framework – Exchange Reference Supplement*, and *Minimum Acceptable Risk Standards for Exchanges – Exchange Reference Architecture Supplement,* 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. Together, these documents, along with the four documents in the ACA System Security Plan Document Suite,[1] 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.

As noted in the *Minimum Acceptable Risk Standards for Exchanges,* this Catalog presents those minimum security controls essential to execution of its guidance. CMS has reviewed and accepted this *Catalog of Minimum Acceptable Risk Controls for Exchanges* as a component of the Exchange Reference Architecture in accordance with the CMS IT governance process.

CMS has circulated this document for review by the following signatory federal partner agencies that share data with the Exchanges through the CMS Data Services Hub. Each agency concurs with the MARS-E Suite guidance, as demonstrated by signature ("/s/") of the authorized signatories for each federal partner agency.

Any changes to this *Catalog of Minimum Acceptable Risk Controls 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.

[1] 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*, Workbook; and *ACA Internal Revenue Service Safeguard Procedures Report Template*.

Introduction

The Patient Protection and Affordable Care Act of 2010[2] (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 to 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.

The Department of Health and Human Services (HHS) and the Centers for Medicare & Medicaid Services (CMS) are responsible for providing guidance and oversight for the Exchanges and for state 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. CMS will focus this guidance on the key tradeoffs and technology choices necessary to create interoperable and coordinated IT services between the federal government and the Exchanges.

1.1 *Purpose*

Protecting and ensuring the confidentiality, integrity, and availability for Exchange 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. This *Catalog of Minimum Security Controls for Exchanges – Exchange Reference Architecture Supplement* (hereafter simply "MARS-E") defines a set of security controls that focuses on the most common vulnerabilities hackers use to exploit systems.

The purpose of this supplement is to augment the security guidance for use by the Exchanges 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, and for documenting the control implementation details in the Exchange's System Security Plan (SSP). Exchanges also are required to define system risks in an Information Security (IS) Risk Assessment (RA).

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, 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 (HITECH). When Exchanges handle Protected Health Information (PHI), they are subject to these laws. In addition, when the

[2] 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

Exchanges carry out business functions that require data sources provided by federal or state entities, each of the data sharing instances carries obligations for protecting the security and privacy of the shared data based on owner specifications. For instance, Internal Revenue Code (IRC) 26 U.S.C. §6103 applies if an Exchange IT system receives Federal Tax Information (FTI). Therefore, Exchanges must develop their IT systems to comply with these standards when applicable. The guidance in this supplement neither relieves nor waives any other federal, state, or other applicable laws, guidance, policies, or standards.

1.2 *Scope*

This document identifies the set of Minimum Security Controls for state IT systems for which CMS has oversight responsibility, starting with Exchanges and common program enrollment systems as required by the Affordable Care Act. The Minimum Security Controls identified in this supplement assume that the applicable state IT system is classified as Moderate and contains Personally Identifiable Information (PII).

1.3 *Taxonomy of this Catalog*

CMS has organized the catalog to present CMS's prescribed Minimum Security Controls into 19 control families within three classes (management, operational, and technical) to provide ease of use. CMS adopted the families in accordance with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*.

Each family contains security controls related to the security functionality of the family. A two-character identifier is assigned to uniquely identify each of the security control families. Some of the controls within a family may have characteristics that can be in more than one class. The class predominantly supported by the family is the class designation for the entire family. Table 1 summarizes the security control families and the two-character identifier used in this catalog.

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.

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.
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.

Family (and Identifier)	Class	Description
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

1.4 *Intended Audience*

The Catalog of Minimum Acceptable Risk Controls for Exchanges – Exchange Reference Architecture Supplement provides details on the Minimum Acceptable Risk Controls for Exchanges for use in the design, implementation, operation, and maintenance of the Exchange IT systems for which CMS has oversight responsibility, and has received the explicit approval of the CMS Deputy Chief Information Officer (DCIO), CMS Chief Information Security Officer, and CMS Chief Technology Officer. 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.

1.5 *Relationship to Other Documents*

The *Catalog of Minimum Acceptable Risk Controls for Exchanges – Exchange Reference Architecture Supplement* must be read in conjunction with the companion *Minimum Acceptable Risk Standards for Exchanges – Exchange Reference Architecture Supplement* and the List of References presented in that document.

1.6 *Document Organization*

The following 19 sections present the descriptions of the specific minimum security controls by Family and Class.

Physical and Environmental Protection (PE) – Operational

Table 150. PE-1: Physical and Environmental Protection Policy and Procedures

PE-1: Physical and Environmental Protection Policy and Procedures		
Control		
The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days: a. A formal, documented physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.		
Guidance		
This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the physical and environmental protection family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The physical and environmental protection policy can be included as part of the general information security policy for the organization. Physical and environmental protection procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the physical and environmental protection policy.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 4.2	**Related Control Requirements:** PM-9
Assessment Procedure: PE-1.1		
Assessment Objective		
Determine if:		
(i) the organization develops and formally documents physical and environmental protection policy; (ii) the organization physical and environmental protection policy addresses: - purpose; - scope; - roles and responsibilities; - management commitment; - coordination among organizational entities; and - compliance; (iii) the organization disseminates formal documented physical and environmental protection policy to elements within the organization having associated physical and environmental protection roles and responsibilities; (iv) the organization develops and formally documents physical and environmental protection procedures; (v) the organization physical and environmental protection procedures facilitate implementation of the physical and environmental protection policy and associated physical and environmental protection controls; and (vi) the organization disseminates formal documented physical and environmental protection procedures to elements within the organization having associated physical and environmental protection roles and responsibilities.		
Assessment Methods and Objects		
Examine: Physical and environmental protection policy and procedures; other relevant documents or records.		
Interview: Organizational personnel with physical and environmental protection responsibilities.		

Table 151. PE-2: Physical Access Authorizations

PE-2: Physical Access Authorizations

Control

The organization:

a. Develops and keeps current a list of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible);

b. Issues authorization credentials;

c. Reviews and approves the access list and authorization credentials in accordance with the frequency specified in Implementation Standard 1, removing from the access list personnel no longer requiring access.

For FTI: A visitor access log containing specific data elements will be used to authenticate and authorize visitor's access to any facility where FTI resides, either electronically or in paper, at the location where the outside (2nd) barrier is breached.

Implementation Standards

1. Review and approve lists of personnel with authorized access to facilities containing information systems at least once every one hundred eighty (180) days.
2. (For PII only) Create a restricted area, security room, or locked room to control access to areas containing PII. These areas will be controlled accordingly.

Guidance

Authorization credentials include, for example, badges, identification cards, and smart cards.

Applicability: Exchanges	**Reference(s):** IRS-1075: 4.3.2	**Related Control Requirements:** PE-3, PE-4

Assessment Procedure: PE-2.1

Assessment Objective

Determine if:

(i) the organization identifies areas within the facility that are publicly accessible;
(ii) the organization develops and keeps current lists of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible); and
(iii) the organization issues authorization credentials (e.g., badges, identification cards, smart cards).

Assessment Methods and Objects

Examine: Physical and environmental protection policy; procedures addressing physical access authorizations; authorized personnel access list; authorization credentials; list of areas that are publicly accessible; other relevant documents or records.

Assessment Procedure: PE-2.2

Assessment Objective

Determine if:

(i) the organization defines the frequency for review and approval of the physical access list and authorization credentials for the facility;
(ii) organization reviews and approves the access list and authorization credentials in accordance with the organization-defined frequency; and
(iii) the organization removes from the access list personnel no longer requiring access.

Assessment Methods and Objects

Examine: Physical and environmental protection policy; procedures addressing physical access authorizations; security plan; authorized personnel access list; authorization credentials; other relevant documents or records.

Table 152. PE-3: Physical Access Control

PE-3: Physical Access Control

Control

The organization:

a. Enforces physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the information system resides (excluding those areas within the facility officially designated as publicly accessible);

b. Verifies individual access authorizations before granting access to the facility;

c Controls entry to the facility containing the information system using physical access devices and/or guards;

d. Controls access to areas officially designated as publicly accessible in accordance with the organization's assessment of risk;

e. Secures keys, combinations, and other physical access devices;

f. Inventories physical access devices within every three hundred sixty-five (365) days; and

g. Changes combinations and keys when keys are lost, combinations are compromised, or individuals are transferred or terminated.

For FTI:

h. Minimum protection standards require two physical barriers between FTI and an individual not authorized to access FTI. This may be achieved through secured perimeter/locked container, locked perimeter/secured interior or locked perimeter/security container. FTI must be containerized in areas where other than authorized employees or authorized contractors may have access after-hours.

i. A security guard, custodial services worker or landlord may have access to a locked building or a locked room if FTI is in a locked container. If FTI is in a locked room, but not in a locked container, the guard, janitor or landlord may have a key to the building but not to the room.

j. During business hours, if authorized personnel serve as the second barrier between FTI and unauthorized individuals, the authorized personnel must wear an identification badge or credential clearly displayed, preferably work above the waist.

k. Unauthorized access to areas containing FTI during duty and non-duty hours must be denied. This can be done utilizing a combination of methods: secured or locked perimeter, secured area or containerization.

l. The physical security and control of computers and electronic media must be addressed. Computer operations must be in a secure area with restricted access.

Guidance

The organization determines the types of guards needed, for example, professional physical security staff or other personnel such as administrative staff or information system users, as deemed appropriate. Physical access devices include, for example, keys, locks, combinations, and card readers. Workstations and associated peripherals connected to (and part of) an organizational information system may be located in areas designated as publicly accessible with access to such devices being safeguarded.

Applicability: Exchanges	**Reference(s):** IRS-1075: 4.2, 4.3, 4.6	**Related Control Requirements:** MP-2, MP-4, PE-2

Assessment Procedure: PE-3.1

Assessment Objective

Determine if:

(i) the organization enforces physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the information system resides (excluding those areas within the facility officially designated as publicly accessible);

(ii) the organization verifies individual access authorizations before granting access to the facility;

(iii) the organization controls entry to the facility containing the information system using physical access devices (e.g., keys, locks, combinations, card readers) and/or guards;

(iv) the organization controls access to areas officially designated as publicly accessible in accordance with the organization's assessment of risk; and

(v) the organization secures keys, combinations, and other physical access devices.

PE-3: Physical Access Control
Assessment Methods and Objects
Examine: Physical and environmental protection policy; procedures addressing physical access control; physical access control logs or records; information system entry and exit points; storage locations for physical access devices; other relevant documents or records.
Interview: Organizational personnel with physical access control responsibilities.
Assessment Procedure: PE-3.2
Assessment Objective
Determine if:
(i) the organization defines the frequency for conducting inventories of physical access devices; (ii) the organization inventories physical access devices in accordance with the organization-defined frequency; (iii) the organization defines the frequency of changes to combinations and keys; and (iv) the organization changes combinations and keys in accordance with the organization-defined frequency, and when keys are lost, combinations are compromised, or individuals are transferred or terminated.
Assessment Methods and Objects
Examine: Physical and environmental protection policy; procedures addressing physical access control; security plan; physical access control logs or records; inventory records of physical access devices; records of key and lock combination changes; storage locations for physical access devices; other relevant documents or records.

Table 153. PE-4: Access Control for Transmission Medium

<table>
<tr><th colspan="3">PE-4: Access Control for Transmission Medium</th></tr>
<tr><td colspan="3"><b>Control</b></td></tr>
<tr><td colspan="3">The organization controls physical access to information system distribution and transmission lines within organizational facilities.</td></tr>
<tr><td colspan="3"><b>Implementation Standards</b></td></tr>
<tr><td colspan="3">1. Permit access to telephone closets and information system distribution and transmission lines within organizational facilities only to authorized personnel.
2. Disable any physical ports (e.g., wiring closets, patch panels) not in use.</td></tr>
<tr><td colspan="3"><b>Guidance</b></td></tr>
<tr><td colspan="3">Physical protections applied to information system distribution and transmission lines help prevent accidental damage, disruption, and physical tampering. Additionally, physical protections are necessary to help prevent eavesdropping or in transit modification of unencrypted transmissions. Protective measures to control physical access to information system distribution and transmission lines include: (i) locked wiring closets; (ii) disconnected or locked spare jacks; and/or (iii) protection of cabling by conduit or cable trays.</td></tr>
<tr><td><b>Applicability:</b> Exchanges</td><td><b>Reference(s):</b> IRS-1075: 4.3.2</td><td><b>Related Control Requirements:</b> PE-2</td></tr>
<tr><td colspan="3"><b>Assessment Procedure: PE-4.1</b></td></tr>
<tr><td colspan="3"><b>Assessment Objective</b></td></tr>
<tr><td colspan="3">Determine if the organization controls physical access to information system distribution and transmission lines within organizational facilities.</td></tr>
<tr><td colspan="3"><b>Assessment Methods and Objects</b></td></tr>
<tr><td colspan="3"><b>Examine:</b> Physical and environmental protection policy; procedures addressing access control for transmission medium; information system design documentation; facility communications and wiring diagrams; other relevant documents or records.</td></tr>
</table>

Table 154Table 154. PE-5: Access Control for Output Devices