Centers for Medicare & Medicaid Services

Harmonized Security and Privacy Framework – 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 nationwide health insurance Exchange(s). Exchange Reference Architecture (ERA) supplements will 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 information technology (IT) standards, data safeguards, and requirements. The Centers for Medicare & Medicaid Services (CMS) 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.

This *Harmonized Security and Privacy Framework – Exchange Reference Architecture Supplement* is the first in a series of Exchange Reference Architecture supplements from CMS to introduce and define a risk-based Security and Privacy Framework for use in the design and implementation of the Exchanges. CMS has reviewed and accepted the *Harmonized Security and Privacy Framework* as a foundational component of the Exchange Reference 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 *Minimum Acceptable Risk Standards for Exchanges – Exchange Reference Architecture Supplement* and the *Catalog of Minimum Acceptable Risk Controls for Exchanges – Exchange Reference Architecture Supplement.* Together, these documents, along with the four documents in the Affordable Care Act (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.

Through this ERA supplement, CMS intends to foster a collaborative discussion between the Exchanges and CMS to assure that the *Harmonized Security and Privacy Framework* and the overall Exchange solution provide the necessary and effective security and privacy for the respective systems and data, and which also provide a flexible enough basis to support compliance with other applicable federal and state security and privacy laws and regulations.

Any changes to the Exchange Reference Architecture 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*.

/s/

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

/s/

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

/s/

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

/s/

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 Workbook,* Version 1.0
- *ACA Internal Revenue Service Safeguard Procedures Report Template,* Version 1.0

SEEN AND APPROVED:

Internal Revenue Service

Terence V. Milholland Chief Technology Officer	/s/ Signature	 Date
S. Gina Garza ACIO, Affordable Care Act (PMO)	/s/ Signature	 Date

Social Security Administration

Kelly Croft Deputy Commissioner for Systems and Chief Information Officer	/s/ Signature	 Date
Brad Flick Associate Commissioner and Chief Information Security	/s/ Signature	 Date

Department of Veterans Affairs

Jerry Davis Deputy Assistant Secretary and Chief Information Security Officer	/s/ Signature	 Date
John Oswalt Associate Deputy Assistant Secretary for Policy, Privacy and Incident Response	/s/ Signature	 Date

Department of Homeland Security

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

Department of Defense

Dr. Karen Guice Chief Information Officer	/s/ Signature	 Date
COL Lorraine Breen Acting Chief Information Officer	/s/ Signature	 Date

Peace Corps

Dorine Andrews Chief Information Officer	/s/ Signature	 Date
Falan Memmott Director of IT Security Assurance & Compliance	/s/ Signature	 Date

Office of Personnel Management

Matthew Perry Chief Information Officer	/s/ Signature	 Date
Andy Newton Chief Information Security Officer	/s/ Signature	 Date

Record of Changes

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

CR: Change Request

Table of Contents

List of Tables

1. Introduction

The Centers for Medicare & Medicaid Services (CMS) is responsible for providing business, information, and technical guidance and oversight for the creation of a common baseline and a set of standards for the national health insurance Exchange implementation activities. CMS will focus this guidance on the key tradeoffs and technology choices necessary to create interoperable and coordinated Exchange services.

CMS has undertaken the development of this guidance through the *Exchange Reference Architecture: Foundation Guidance* document, which describes at a high level the Business, Information, and Technical Reference Architectures that comprise the Exchange Reference Architecture (ERA). This document is the first in a series of ERA supplements that provide the necessary detail and guidance for the successful implementation of the Exchange systems.

1.1 Background

The Patient Protection and Affordable Care Act[2] (hereafter simply the "Affordable Care Act" or "ACA") 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 the health insurance Exchanges to obtain comprehensive information on coverage options currently available through the Exchanges, enabling them to make informed health insurance choices as they select coverage. By pooling people together, reducing transaction costs, and increasing transparency, Exchanges create more efficient and competitive health insurance markets for individuals and small employers.

Adoption of strong security and privacy protections is necessary to establishing the public trust. Studies have consistently shown 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.

The frequency of IT-related attacks on our health care systems is increasing. Cybercriminals see greater incentives in stealing medical information rather than credit card numbers ("street" resale value is claimed to be $50 per health care client record versus $1 per credit card number). With the adoption of Electronic Healthcare Record (EHR) portals and systems where PII and PHI are stored or exchanged, the cybercriminal will have even more opportunities to gain access to sensitive health-related data. The complexity of the threats continues to grow while there is a marketplace shortage of qualified cyber security experts to secure these health IT systems.[3]

The federal government is required by law to protect its IT systems and the information contained within those systems. The federal government also is responsible for ensuring that reasonable IT security and privacy controls are in place for those parties with whom data are shared. There is a complex array of requirements that govern federal and state IT security and privacy. HHS Final Rule on ACA Exchanges contains specifications for safeguarding the Privacy and Security of

[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

[3] Office of Management and Budget (OMB) Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information,* May 22, 2007.

Personally Identifiable Information (PII). Federal agencies and their contractors must adhere to the Federal Information Security Management Act (FISMA) in developing, documenting, and implementing programs to provide security for federal government information and information systems. Both federal and state agencies may be "covered entities" 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), and thus, subject to these laws when handling PHI. These federal agencies and, in some instances, their contractors, are also subject to the Privacy Act of 1974, which places limitations on the collection, disclosure, and use of certain personal information, including PHI. The privacy provisions of the e-Government Act of 2002 require federal agencies to conduct privacy impact assessments (PIA) to assess risks and protections when collecting, maintaining, and disseminating PII. Most, if not all, states also have statutes that protect, in varying degrees, the privacy of PII, including patient health information. In addition, Exchanges and their contractors must adhere to the data safeguard requirements of the Internal Revenue Code, 26 U.S.C. §6103, herein referred to as "Tax Information Safeguarding Requirements," and all corresponding security guidance, as a condition of receiving Federal Tax Information (FTI).

Exchanges must perform certain minimum business functions. These business functions require data from various federal agencies, including the Department of Health and Human Services (HHS), Internal Revenue Service (IRS), Social Security Administration (SSA), and Department of Homeland Security (DHS). Each of these Departments and agencies has unique data protection requirements.

There is no single, integrated, comprehensive approach to security and privacy that respects all potentially applicable federal requirements under FISMA, HIPAA, HITECH, ACA, Tax Information Safeguarding Requirements, and state requirements. Differences in the laws may be in the areas of system categorization, selection of operational security controls, and the use of program management controls. Given the diversity of federal and state laws and regulations governing security and privacy that may apply, CMS developed this *Harmonized Security and Privacy Framework – Exchange Reference Architecture Supplement* to identify key aspects of the security controls required by these laws to provide a flexible basis to support compliance with the applicable laws. Nothing in this document should be construed to eliminate the obligation for an Exchange to comply with the requirements of other applicable privacy and security laws.

1.2 Purpose

The purpose of this *Harmonized Security and Privacy Framework* is to communicate certain key federal guidance and requirements to enable effective Exchange security and privacy implementation and operation. This document addresses the following key security and privacy topics:

1. System and Data Classification
2. Security Controls
3. Identity, Credential, and Access Management
4. Secure Infrastructure and Managed Services Computing
5. Data Encryption
6. Audit Trails
7. Continuity of Operations and Disaster Recovery
8. Compliance Oversight
9. Privacy

1.3 Scope

This *Harmonized Security and Privacy Framework* represents Part 1 (of two parts) of the definition of the Harmonized Security and Privacy Framework, identifying considerations to be addressed (the "what and why"). Another Exchange Reference Architecture Supplement, the *Minimum Acceptable Risk Standards for Exchanges – Exchange Reference Architecture Supplement*, provides detailed definition of a common baseline of minimum acceptable risk controls requirements that will support collaborative solutions to manage risks (the "how").

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

The guidance provided in this document reflects industry and government best practices to support a viable approach for the federal government and the states.

1.4 Intended Audience

The distribution of this document is available to all states, other federal agencies, and supporting contractors.

1.5 Document Organization

This document is organized as follows:

Section		Overview
Section 2:	The Security and Privacy Requirements Landscape	Presents legislative and regulatory security and privacy requirements regarding data classified as PII / PHI, and entity classification of "covered entity" or "business associate".
Section 3:	Risk-Based Security and Privacy Framework Considerations	Presents key considerations of a risk-based Security and Privacy Framework for use in implementing and operating an Exchange.
Appendix A:	Key Laws and Guidance Governing the Exchange of PII and PHI	Provides definition and context to federal laws that bound the Harmonized Security and Privacy Framework.
Acronyms		Defines the acronyms used in this document.
List of References		Lists the references used in preparing this document.

2. The Security and Privacy Requirements Landscape

As indicated above, there are 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 upon federal agencies, state partners, contractors, and supporting commercial companies. These include:

- Federal Information Security Management Act (FISMA) of 2002
- Health Insurance Portability and Accountability Act (HIPAA) of 1996
- Health Information Technology for Economic and Clinical Health Act (HITECH) of 2009
- Privacy Act of 1974
- e-Government Act of 2002
- Patient Protection and Affordable Care Act of 2010
- Safeguards for Protecting Federal Tax Returns and Return Information (26 U.S.C. §6103 and related provisions)

All parties must confront the following issues when defining a risk-based security and privacy framework. This section presents a high-level guide to help address these issues:

- What key federal and state security and privacy laws, regulations, standards, and guidance apply to my system?
- How are entities defined in the context of security and privacy?
- What key technical considerations must be addressed to develop harmonized security and privacy requirements?

This document and future Exchange Reference Architecture supplements should help answer these questions.

2.1 Determining the Applicability of Federal Mandates

2.1.1 Crosswalk of Laws, Required Standards, and Guidance

All federal agencies, and in some cases their contractors, must comply with FISMA, the Privacy Act of 1974, and the e-Government Act of 2002. Certain federal and state agencies, and health care entities must comply with HIPAA and HITECH requirements. Federal and state agencies, as well as contractors, must comply with Tax Information Security Guidelines as a condition of receipt of FTI. Finally, states and other non-federal entities must comply with state laws and regulations.

Table 1 provides a crosswalk of some of the key standards and guidance that may apply to specific entity types. The table shows two major sectors for entities, “Federal” and “non-Federal”. Within each sector, there are designations for HIPAA covered entities (CE), business associates (BA), or “other.”

Table 1. Crosswalk of Certain Key Laws, Standards, Guidance, and Agreements that May Apply

		Entity Type					
		Federal CE	Federal, Non-CE		Non-Federal CE	Non-Federal, Non-CE	
	Appendix Reference		Business Associate	Other		Business Associate	Other
Security and Privacy Laws, Requirements, and Standards	A.1 FISMA	Yes	Yes	Yes	No	No	No
	A.2, A.3) HIPAA & HITECH (1) (2)	Yes	Yes(3)	No	Yes	Yes(3)	No
	A.4 Privacy Act of 1974	Yes	Yes	Yes	No	No	No
	A.5 e-Gov Act of 2002	Yes	Yes	Yes	No	No	No
	A.7 IRC 6103	Yes	Yes	Yes	Yes	Yes	Yes
	State Laws	No	No	No	Yes	Yes	Yes
Other Guidance and Controls	A.1 FIPS 199 and 200	Yes	Yes	Yes	No	No	No
	A.1 NIST Guidance	Yes	Yes	Yes	No	No	No
	A.4 OMB Privacy & Security Guidance	Yes	Yes	Yes	No	No	No
	A.6 Patient Protection and Affordable Care Actand HHS Final Rule	Yes	Yes	Yes	Yes	Yes	Yes
	A.7 IRS Publication 1075	Yes	Yes	Yes	Yes	Yes	Yes
	State Guidance	No	No	No	Yes	Yes	Yes
Key Agreements	A.2 Business Associate Agreement / MOU	Yes(4)	Yes(4)	No	Yes(4)	Yes(4)	No
	Interconnection Security Agreement	Yes	Yes	Yes	Yes	Yes	Yes
	Data Sharing Agreement/Data Use Agreement/ Data Exchange Agreement	Yes	Yes	Yes	Yes	Yes	Yes
	IRS Data Exchange Agreement	Yes	Yes	Yes	Yes	Yes	Yes

(1) The HIPAA Privacy Rule,unlike the Security Rule, applies to PHI in "any form or medium." The Security Rule covers only PHI that is electronically stored or transmitted by covered entities See 45 CFR Parts 160, 162, and 164 at http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/adminsimpregtext.pdf.

(2) The Health Information Technology for Economic and Clinical Health (HITECH) Act was enacted as part of the American Recovery and Reinvestment Act of 2009. HITECH ammends HIPAA to strengthen the privacy and security protections for health information and to improve the workability and effectiveness of the HIPAA Rules. HHS has not finalized all of the regulations that will implement the changes to date; however, final rules are expected sometime in the second quarter of 2012.

(3) The HITECH Act extends the applicability of certain HIPAA Privacy and Security Rule requirements to business associates of covered entities.

(4) There are certain exceptions. See § 164.504(e)(1)(ii).

2.1.2 HIPAA Covered Entities and Business Associates

Federal and non-federal organizations that operate Exchange(s) must determine their entity classification under HIPAA. Organizations must determine whether they are HIPAA covered entities or business associates. Covered entities are health plans, health care clearinghouses, and health care providers that transmit health information 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.

2.1.3 HIPAA Requirements

Organizations that are covered entities under HIPAA or business associates of HIPAA covered entities are required to follow the HIPAA Privacy, Security, and Breach Notification Rules, as applicable, with respect to the PHI they create, receive, maintain, or transmit. Organizations may refer to guidance on the HHS web site to help them determine if they are a HIPAA covered entity or business associate, and what the HIPAA Rules require: www.hhs.gov/ocr/privacy.

2.1.4 Type of Data Created, Collected, Transported, or Processed

The HIPAA Rules apply to most individually identifiable health information created, received, maintained, or transmitted by HIPAA covered entities and their business associates. This is called "protected health information" or PHI. Note that PII and FTI may be PHI to the extent that such information otherwise meets the definition of individually identifiable health information in the HIPAA Rules and is created, collected, maintained, or transmitted by a HIPAA covered entity or business associate. Table 2 provides the controlling definitions for PII, PHI, individually identifiable health information (IIHI), and FTI.

Table 2. Key Data Definitions

Term	Definition
PII	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.
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.
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.
FTI	Generally, federal tax returns and return information are confidential, as required by IRC Section 6103. The IRS uses the IRC to ensure that agencies, bodies, and

Term	Definition
	commissions maintain appropriate safeguards to protect the information confidentiality. (See IRS Publication 1075 reference)

If an Exchange collects or shares aggregate, non-identifiable information to make a risk adjustment calculation, this may not be considered PHI so long as the data has been de-identified in accordance with the HIPAA Rules.

The importance of this is that covered entities and business associates that handle PHI must comply with the HIPAA Privacy and Security Rules with respect to such information. If the information is not considered PHI or if the entity is not a covered entity or business associate, then the HIPAA Privacy and Security Rules do not apply. However, in all cases, a basic level of security and privacy controls is required for information maintained by the Exchange.

2.2 Use of Agreements

The Exchange Reference Architecture: Foundation Guidance document provides a high-level overview of the business, information, and technical architectures of Exchanges. The document confirms that the Exchanges carry out business functions that require data sources provided by federal and state agencies. Each of the data sharing instances carries obligations for protecting the security and privacy of the shared data based on owner specifications. These obligations are usually communicated in the form of business associate agreements, systems interconnection security agreements, and data sharing/data use/data exchange agreements. Section155.260 (e) of the HHS Final Rule on ACA provides explicit requirements for data sharing arrangements.

2.3 Other Considerations

Non-federal entities must abide by state laws for information sharing, and those statutory requirements vary considerably.

IRS Publication 1075, *Tax Information Security Guidelines for Federal, State, and Local Agencies and Entities*, contains detailed guidance on security measures needed to safeguard federal tax information under Internal Revenue Code (IRC) 26 U.S.C. §6103.

When faced with conflicting federal and state requirements, the Exchange systems must follow the most stringent requirement.

3. Risk-Based Security and Privacy Framework Considerations

Section 1561 of the Affordable Care Act requires the 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. Section 155.260 of the HHS Final Rule on ACA requires Exchanges to establish and implement privacy and security standards consistent with the principles stipulated in the Rule. CMS will work with Exchange stakeholders to define a risk-based Harmonized Security and Privacy Framework. The framework will include standard methods to classify systems and data relative to risk, and a minimum set of privacy measures and critical security controls required for the protection of such systems and data, while ensuring compliance with federal and state laws and regulations. In parallel with guidance provided in this document, system owners should follow general guidance for managing risk in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems.*

The Harmonized Security and Privacy Framework is intended to guide Exchange stakeholders in making appropriate architecture and design decisions. The framework will instruct Exchange stakeholders how to assess system and data sensitivity, and their risk exposure in the context of Exchange business processes. Implementers will use the framework to guide their architectural decisions for the implementation and operation of the Exchange systems, and in support of other initiatives involving the development of policies, processes, procedures, and agreements for appropriately safeguarding systems and data shared with other entities. The Harmonized Security and Privacy Framework will identify requirements (including legislation, policies, standards, guidance, controls, and agreements) as well as options for making risk-based decisions and addressing any limitations and gaps.

PII and PHI are two types of data of particular concern for Exchange systems. In addition, the Exchanges will also transmit and/or process individuals' financial information, including FTI, as required to support Exchange business processes.

Having a common and Harmonized Security and Privacy Framework will improve efficiencies with Exchange system definition, implementation, and operation. A common framework will also facilitate compliance and oversight services. The greatest benefit of the framework will be to minimize the risks of security and privacy vulnerabilities.

Initial security and privacy controls to be considered in the Harmonized Security and Privacy Framework are:

1. System and Data Classification
2. Security Controls
3. Identity, Credential, and Access Management
4. Secure Infrastructure and Managed Services Computing
5. Data Encryption
6. Audit Trails
7. Continuity of Operations and Disaster Recovery
8. Compliance Oversight
9. Privacy

The following subsections address each of these controls.

3.1 System and Data Classification

The federal government has adopted standards to classify IT data and systems security (Low, Moderate, and High) and has established a catalog of security controls that are required at each level. NIST Federal Information Processing Standards (FIPS) Publication (Pub) 199, *Standards for Security Categorization of Federal Information and Information Systems,* describes this approach. CMS recommends that Exchanges follow this process.

FIPS 199 establishes security categories for both data and systems. First, data that are considered sensitive are identified and categorized according to information type. An information type is a specific category of information (e.g., medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an entity or, in some instances, by a specific law, Executive Order, directive, policy, or regulation. Next, security categorization is performed based upon the potential impact on the entity (or a community of entities) should a breach of security occur (i.e., a loss of confidentiality, integrity, or availability). The classification of IT data and systems security in FIPS Pub 199 is as follows:

- The potential impact is *Low* if the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on entity's operations, organizational assets, or individuals.
- The potential impact is *Moderate* if the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on the entity's operations, organizational assets, or individuals.
- The potential impact is *High* if the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on the entity's operations, organizational assets, or individuals.

Exchange implementers will find NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories,* a helpful reference for performing the categorization tasks.

Best practice is for all Exchange stakeholders to consider the data classifications specific to their systems and the resulting system classifications. For example any system classified as "Moderate" by virtue of processing PHI would retain at least the "Moderate" classification if the system began to process PII data. Similarly, in order for a system classified as "Low" to exchange data with a "Moderate" system, the "Low" system might be required to meet moderate-level security transmission requirements.

FIPS Pub 200, *Minimum Security Requirements for Federal Information and Information Systems,* along with NIST SP 800-53, *Recommended Security Controls for Federal Information Systems,* specifies minimum data security requirements (i.e., management, operational, and technical controls), for data and data systems in each such security category. The strength of security controls required is commensurate with the security categorization level of the system.

Security categorization standards provide a common framework that enables:

- Effective management and oversight of information security programs, including the coordination of information security efforts among all stakeholders, and
- A consistent way of measuring the adequacies of information security policies, procedures, and practices.

Systems that contain federal tax information are deemed moderate risk.

3.2 Security Controls

The Harmonized Security and Privacy Framework will identify security controls commensurate with the sensitivity of the data stored and exchanged. This will allow Exchange implementers to prioritize architectural and design security and privacy decisions in areas that present the greatest risk to the Exchange solution.

To help accelerate the creation of appropriately secure IT systems that support Exchange and common program enrollment systems, CMS is providing a Minimum Acceptable Risk Standards for Exchanges, which identifies a minimal set of critical controls that must be adopted by all entities implementing and operating Exchanges. The Exchanges will need to implement these controls in conjunction with the applicable requirements of HIPAA, HITECH, ACA, FISMA, and FTI.

3.3 Identity, Credential, and Access Management

Controlling access to systems that contain PII, PHI, or FTI is paramount to ensuring the security and privacy of a person's medical and personal information. There are many technical considerations that must be addressed successfully to implement data sharing on a wide scale across federal and non-federal entities. For example, without the appropriate vetting of user identities' and proper access controls, unauthorized users can obtain PII, PHI, or FTI data. Systems that contain this type of data tend to be targets for theft of medical information and patient or provider identities. To ensure proper security access, Exchange entities must implement the appropriate constructs to identify, verify, authorize, and authenticate users before allowing access to sensitive resources.

The architecture and design of Exchange systems must address a range of administrative and technical considerations. Given the large population of users and the number of different business entities involved in the use and operations of the Exchanges, the Harmonized Security and Privacy Framework will address a comprehensive approach toward roles and responsibilities for providing Exchange Identity, Credential, and Access Management (ICAM) services. One possible model for consideration is the Federal Identity, Credential and Access Management model introduced by the Federal CIO Council.

Closely related to authentication and credentials are the requirements for accountability and non-repudiation. Non-repudiation should be required for only the most critical transactions.

The following principles should apply to the ICAM for all Exchange systems:

- **Identity proofing.** Provide a minimum set of administrative controls and requirements for identity proofing (validating that users are who they say they are) and for the periodic management of authenticators.

- **Authorization.** Users will be assigned roles to ensure that they only have access to data that is needed to get the job done and nothing more (least privilege). The Harmonized Security and Privacy Framework will provide a minimum set of roles for implementation by all Exchanges. The framework will also address a minimum set of supporting processes, and the authorization rights and steps required to grant access to such resources.

- **Authentication.** A best practice is to require increasing complexity of authentication as the sensitivity of the system and data increases. The Harmonized Security and Privacy Framework will provide guidance regarding what type of authentication will be required based on the sensitivity of data processed within the Exchange.

3.4 Secure Infrastructure and Managed Services Computing

Implementing a defense-in-depth computing architecture is a good way to manage risk. Defense-in-depth means that the computing architecture depends upon multiple layers of security; each layer is protected by a suite of security devices—often from different vendors—to increase the strength of the security infrastructure. Each layer will offer a limited number of services, ports, and protocols, which restricts the ability to subvert the layer.

A best-practice, defense-in-depth computing architecture is a multi-zone architecture that physically separates the layers between system components. The Presentation Zone is separate from the Application Zone, which is separate from the Data Zone. Architecture frameworks, like the Medicaid Information Technology Architecture (MITA),[4] recommend such a zoned architecture, with each zone protected by firewalls and intrusion detection devices.

The Federal Chief Information Officer's recent publication, *25 Point Implementation Plan to Reform Federal Information Technology Management*, emphasizes the shift to a "cloud first" policy for federal IT developments. As a result, government agencies are adopting cloud computing; however, the security of the cloud remains a key open issue. There are evolving cloud security considerations, such as the Federal Risk and Authorization Management Program (FedRAMP), which eventually will become standard baselines for defining cloud security. NIST, for example, clearly defines Public, Community, and Private clouds. In this sequence of cloud models, each subsequent type allows stricter security and architecture definition and control by the implementing organization. *Public* clouds generally use the public Internet for all access and information exchange; employ servers and data storage devices that are shared between customers; and leave security definition, implementation, and management up to each customer. *Private* clouds are generally built to the customer's specification, including definition of the security infrastructure, variety in vendor devices, and dedicated servers and storage.

Best practices by an Exchange stakeholder are to evaluate the system and data classification for the Exchange, determine the level of risk the stakeholder will manage, and define an appropriate managed services model that will support the implementation of a multi-zone architecture and a secure infrastructure.

CMS intends to support a managed services implementation. In addition, the guidance in future Exchange Reference Architecture supplements will define the use of managed services-based technical environments for the Exchanges.

[4] For MITA definition, see https://www.cms.gov/MedicaidInfoTechArch/04_MITAFramework.asp

3.5 Data Encryption

Implementation of data encryption can offer protection of data confidentiality and integrity when used correctly; however, it is not without cost, both in terms of computing cycles and key management expenses. Encrypting or not must be a risk-based decision that considers the sensitivity of the data, the threat level (likelihood of compromise in a defense-in-depth environment), and the severity of impact in the event of a security compromise.

The Harmonized Security and Privacy Framework will address such data encryption topics as:

- Sensitive data in transit (including e-mail) that requires confidentiality protection will be encrypted when traversing entity boundaries. For data in transit where the only concern is the protection of integrity, hashing techniques and message authentication codes may be used instead of encryption. IRS guidance calls for the encryption of FTI data while it traverses within the entity. If encryption is not used for FTI, the entity must use other compensating mechanisms—e.g., switched Virtual Local Area Network (VLAN) technology, fiber optic medium, etc.—to ensure that FTI is not accessible to unauthorized users.
- Portable storage media. Off-site backup data will be encrypted when not under the control of the Exchanges. Data residing on removable storage media or devices will be encrypted.
- Only FIPS Pub 140-2-approved (or higher) encryption algorithms will be used.
- If an entity uses Public Key Infrastructure (PKI), the entity will follow standard practices such as the use of accepted certification authorities, documented Certificate Policy (CP), and Certification Practice Statement (CPS), which will include key escrow strategy. Implementation will use foundational technical standards such as X.509 Certificate format and Public Key Cryptography Standard (PKCS).
- If PKI is used across entities, interoperability requirements must be addressed.

3.6 Audit Trails

Properly implemented, audit trails provide for accountability and non-repudiation, ensuring that the organization can trace actions on the system back to the responsible individuals.

The Harmonized Security and Privacy Framework will address such audit trail topics as determining:

- The minimum set of events and/or transactions that must be logged
- Data capture and storage requirements
- Review, reporting, and analysis requirements
- Log/audit data retention and archival requirements

Audit logs may also facilitate implementation of other security and privacy requirements, for example:

- Audit trails may enable periodic risk analysis to prevent, detect and contain potential security violations and protect PHI, as required by HITECH[5]

[5] 45 C.F.R. § 164.308(a)(i)(1)

- Audit trails may be used to enable tracking of unauthorized disclosures of FTI or PHI[6]

Audit trails can serve a useful role in recreating a security incident and determining the extent of a security breach. This will in turn allow the covered entity to respond and report appropriately. For example, good audit trails can help identify the number of individual records affected by a breach. This accurate data can affect the number of individuals who must be notified and affect the impact of civil penalties. When a covered entity does not have good audit trails, the entity is at greater risk of having to notify *all* individuals because the entity does not know how many records were accessed or leaked during a breach.

3.7 Continuity of Operations and Disaster Recovery

Maintaining continuity of service for the Exchange consumer is of utmost importance. This drives the need for Exchange operators to establish strategies and plans for maintaining continuity of operations of critical services (even if these services must be in degraded or manual mode) when some system components are out of service, and systematic restoration of service following a system disaster.

In addition, certain Security and Privacy Framework considerations must be addressed in the planning and design of system infrastructure, configuration, and operations to minimize loss and facilitate effective disaster recovery. The following considerations are critical:

- Adhere to the principle of "Fail Safe" to ensure that a system in a failed state does not reveal any sensitive information or leave any access controls open for attacks
- Use fully redundant network and hardware. Hardware components (such as processor and memory) should have built-in redundancy to allow a second component to take over in the event of a failure in the primary component. Similarly, redundant paths should also exist for networks.
- Use offsite storage. Data backup should be stored offsite in the event of a physical disaster.
- Build in contingencies for the storage of transactions where there is dependency on availability of data from business partners that provide authoritative data (e.g., the IRS, DHS, and SSA). The Exchange requirements will include identification of data availability requirements.
- Leverage virtualization to expedite disaster recovery. Virtualization enables system owners to quickly reconfigure system platforms without having to acquire additional hardware.

3.8 Compliance Oversight

In order to maintain consumer confidence and stakeholder trust, it is critical to include security and privacy oversight within the operations governance for the Exchanges. Section 1411(g) of the Affordable Care Act specified the need to protect the confidentiality of PII in Exchange-related processes, and §155.260 of the HHS ACA Final Rule specified the requirements for privacy and security. Exchanges can be operated by a state agency, quasi-governmental agency, or a non-profit entity. Exchanges must comply with applicable federal and state laws and regulations,

[6] The HIPAA Privacy Rule allows an individual to request a written record of disclosures of their PHI made by a covered entity; see CMH OCR "Personal Health Records and the HIPAA Privacy Rule" at http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/phrs.pdf

internal policies of the Exchanges, as well as any business partner agreement (with individual data sharing entities and health insurance entities). Any data exchanged between entities as part of Exchange implementation or operation will require a governing data use agreement or data exchange agreement, whereby each entity assumes responsibility for ensuring protection of transmitted data once received. Exchanges are also required to protect PII from unlawful use.

The federal government will monitor the Exchange operations in accordance with FISMA Continuous Monitoring guidelines, and will ensure compliance with any federal-level data use agreements and information exchange agreements among federal partners. CMS will establish Interconnection Security Agreements with federal and non-federal partners to ensure security requirements are met by all entities connecting to the federal ACA system.

It is recommended that each Exchange owner establish an IT governance body and appoint an accountable individual who has oversight responsibility of IT security and privacy activities.

Health insurance companies and other business entities undergo a “sign-on” process to engage in Exchange activities. As part of the sign-on process, each entity will agree to take on the security and privacy responsibilities of a business partner. Each business partner will appoint an individual who has oversight responsibility of IT security and privacy activities.

Each Exchange owner is responsible for conducting the baseline oversight activities. These oversight activities include:

- Ensuring risk management is performed in accordance with NIST SP 800-37 guidance
- Documenting policies and procedures, based on applicable laws, governing the collection, use, and disclosure of PII
- Ensuring systems are developed following System Development Life Cycle (SDLC) best practices and secure coding practices to avoid common software weakness and vulnerabilities
- Ensuring the documentation of necessary and appropriate security and privacy artifacts
- Serving as approval authority for the systems and interconnections
- Enforcing ongoing monitoring and periodic compliance reporting, and providing evidence on the compliance levels of security and privacy requirements, data exchange agreements, and data use agreements
- Conducting system assessments

The goal of a security assessment (also known as a security audit or security review) is to ensure that necessary security controls are integrated into the SDLC of a project and incorporated into the production system. A properly completed security assessment should provide documentation delineating any security gaps between a project’s designs and approved security policies. Periodic assessments will assure continuous compliance when systems are deployed.

3.9 Privacy

Building appropriate privacy protections into the design of the Exchanges will be crucial to gaining the necessary public trust to make them successful. It is important to note that the terms privacy and security are not synonymous. While privacy focuses on the individual’s ability to control the collection, use, dissemination, and disposition (when no longer needed) of their PII, security provides the mechanisms to ensure confidentiality and integrity of information, and the availability

of IT systems. Adequate security controls help protect an individual's privacy, but are insufficient protection on their own—they must work in conjunction with the individual's ability to control access to their PII.

HHS has recognized the importance of incorporating privacy and security into its efforts to encourage health information exchange. As a result, in 2008, it established a harmonized framework of privacy and security principles to address the privacy and security challenges related to electronic health information exchange. Section 155.260 of the HHS Final Rule on ACA Exchanges contains the eight privacy principles and a set of minimum requirements of safeguarding the privacy of Exchange related PII:

- **Individual Access:** Individuals should be provided with a simple and timely means to access and obtain their personal health 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 health information, and to have erroneous information corrected or to 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 health 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 health information.
- **Collection, Use, and Disclosure Limitation:** Individually identifiable health information should be collected, used, and/or disclosed only to the extent necessary to accomplish a specified purpose(s) and never to discriminate inappropriately.
- **Data Integrity:** Persons and entities should take reasonable steps to ensure that individually identifiable health 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 health 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.

Exchanges must establish and implement privacy and security standards that are consistent with these principles. Exchanges must establish and implement operational, technical, administrative, and physical safeguards that are consistent with any applicable federal laws and standards to ensure the confidentiality, integrity, and availability of PII created, collected, used, and/or disclosed by the Exchanges. This includes ensuring that PII is securely destroyed or disposed of, and in accordance with retention schedules. Exchanges must also ensure that their workforce complies with the policies and procedures developed and implemented by the Exchange to adhere to with these principles.

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 gain access to PII submitted to an Exchange; or collect, use or disclose PII gathered directly from

applicants, qualified individuals, or enrollees while that individual or entity is performing the functions outlined in the agreement with the Exchange.

Personally identifiable information should only used by or disclosed to those authorized to receive or view it. HIPAA, ACA, and state law, as applicable, also provide specific requirements regarding the implementation of these principles. Where an Exchange creates or collects PII for the purposes of determining eligibility for enrollment in a qualified health plan, the Exchange may not create, collect, use, or disclose PII unless consistent with the principles in this section.

Both the federal government and the Exchanges should consider how these principles will be built into the processes and IT systems. . For example:

- Policies, processes, and procedures should be established to allow individuals access to their own information held by the Exchanges, and to request corrections as appropriate.
- Policies, processes, and procedures should allow for the disposition of PII data when no longer needed, as well as retention schedules for this data.
- IT systems should include the capability to retrieve an individual's information and present it in an understandable format.
- Consumers should be provided with clear notice of what information is being collected by the Exchanges, the purpose of the collection, and how the information is to be used and shared.

Appendix A. Key Laws and Guidance Governing the Exchange of PII and PHI, and the Disclosure of FTI

There is no single federal law that governs all uses or disclosures of both Personally Identifiable Information (PII) and Protected Health Information (PHI). 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 and PHI, as well as guidance governing the disclosure of Federal Tax Information (FTI).

A.1 The Federal Information Security Management Act of 2002

The Federal Information Security Management 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, *Recommended Security Controls for Federal Information Systems*.** This publication provides guidelines for selecting and specifying security controls for information systems supporting the federal government.

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 management, operational, and technical 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.

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, 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 Health Insurance Portability and Accountability Act of 1996

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) provides for the protection of most individually identifiable health information held by covered entities, defined as health plans that provide or pay for the medical care of individuals, health care providers that electronically transmit health information in connection with any of the specific transactions regulated by the statute, and healthcare clearinghouses that receive health information from other entities and process or facilitate the processing of that information into standard or non-standard format for those entities. The law provided for the Secretary of HHS to establish the first broadly applicable federal privacy and security protections designed to protect individual health care information.

The Secretary of HHS first issued HIPAA's Privacy Rule in December 2000, following public notice and comment, but later modified the rule in August 2002. The Privacy Rule governs the use and disclosure of PHI, which is generally defined as Individually Identifiable Health Information that is held or transmitted in any form or medium by a covered entity. A covered entity must disclose PHI in only two situations: (1) to individuals specifically when they request access to, or an accounting of disclosures of, their PHI, and (2) to HHS when it is conducting a compliance investigation or enforcement action. Generally, covered entities are permitted (but not required) to disclose PHI to other entities for purposes of treatment, payment, and health care operations without an individual's authorization. Covered entities may also disclose PHI, without an individual's authorization, for certain other permitted uses and disclosures specified in the rule. These permitted uses and disclosures include those for certain public interest and benefits activities, such as for law enforcement, judicial, and public health, provided certain conditions are met. All other uses and disclosures not otherwise permitted by the Privacy Rule require an individual's written authorization. In addition, the Privacy Rule requires that a covered entity make

reasonable efforts to use, disclose, or request only the minimum necessary protected health information to accomplish the intended purpose, with certain exceptions such as for disclosures to health care providers for treatment, and uses and disclosures required by law.

Subsequent to the issuance of the Privacy Rule, the Secretary issued the HIPAA Security Rule in February 2003 to safeguard electronic protected health information and help ensure that covered entities have proper security controls in place to provide assurance that the information is protected from unwarranted or unintentional disclosure. The Security Rule includes administrative, physical, and technical safeguards and specific implementation instructions, some of which are required and, therefore, must be implemented by covered entities. Other implementation specifications are "addressable" and, under certain conditions, permit covered entities to use reasonable and appropriate alternative steps. Covered entities are required to develop policies and procedures for both required and addressable specifications. NIST SP 800-66, Revision 1, *An Introductory Resource Guide for Implementing the HIPAA Security Rule,* provides guidance on security considerations and resources for implementing the requirements of the Security Rule.

HIPAA provides authority to the Secretary to enforce these standards. The Secretary has delegated administration and enforcement of the HIPAA Privacy and Security Rules to the Department's Office for Civil Rights (OCR). Individuals who believe that their PHI has been improperly handled may file a complaint with OCR, which is authorized to investigate the matter.

In 2009 the HIPAA law changed as a result of the passage of the Health Information Technology for Economic and Clinical Health Act (HITECH Act).[7] The HITECH Act expands the authority to sue by authorizing state attorneys general to file civil suits on behalf of their residents for HIPAA violations.[8]

Individuals who believe that their PHI has been improperly handled may file a complaint with the HHS Department Office for Civil Rights (OCR) and/or the state attorney general's office of the state in which he/she resides.[9] These entities are authorized to investigate the matter.

An important concept under the Privacy and Security Rules is that of "business associate." The HIPAA Rules generally define a "business associate" as an entity, other than a member of a covered entity's workforce, that performs certain functions or activities on behalf of, or provides certain services to, a covered entity that involve the use or disclosure of PHI.[10] Business associate functions on behalf of a covered entity include claims processing, data analysis, utilization review, and billing. Business associate services to a covered entity are limited to legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services. (A covered entity can be the business associate of another covered entity.) When using a contractor or other non-workforce member to perform such functions or services, a covered entity must obtain—through a formal "business associate agreement"—satisfactory assurances that its business associates will appropriately safeguard protected health information. The Security Rule also contains specific requirements for business associate contracts and requires that covered entities maintain compliance policies and procedures in written form. Thus, the agreement makes the business associate, who is not a covered entity, subject to the privacy and security requirements in the rules.

---

7 The HITECH Act, §13410.

8 HHS, OCR, "How to File a Complaint", *at* http://www.hhs.gov/ocr/privacy/hipaa/complaints/index.html

9 If the HHS Secretary has instituted an action against a person for a HIPAA violation, no state attorney general may bring an action against the person while the HHS-led action is pending. *See* The HITECH Act, §13410.

10 The HITECH Act modifies HIPAA to strengthen the privacy and security protections for health information and to improve the workability and effectiveness of the HIPAA Rules. HHS has not finalized all of the regulations that will substantively change the HIPAA to date, but final rules are expected sometime in the second quarter of 2012.

Where before business associates were only contractually liable for misuses of PHI or failures to adequately safeguard PHI, the HITECH Act makes business associates of covered entities directly liable for making a use or disclosure of PHI in violation of the Privacy Rule or its business associate contract and for failing to comply with the Security Rule. The Department will issue final rules to implement these expanded liability provisions.

In general, the provisions of state laws that run contrary to the Privacy and Security Rules are preempted by the federal requirements, and thus, the federal requirements will apply. The HIPAA Rules provide certain exceptions to this general rule of federal preemption of contrary state laws for state laws that (1) relate to the privacy of individually identifiable information and provide greater privacy protections or privacy rights with respect to such information; (2) provide for the reporting of disease or injury, child abuse, birth, or death, or for public health surveillance, investigation or intervention; or (3) require certain health plan reporting, such as for management or financial audits. In addition, the HIPAA Rules provides a process for HHS to make exception determinations in certain cases.

A.3 The Health Information Technology for Economic and Clinical Health Act of 2009

The Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH) is part of the American Recovery and Reinvestment Act of 2009 (ARRA). ARRA contains incentives related to health care information technology in general (e.g., creation of a national health care infrastructure). HITECH strengthens privacy and security protections available under HIPAA by, for example, extending liability for compliance with certain provisions of the HIPAA Rules directly to business associates and increasing the civil money penalties that may be imposed for non-compliance.

Of particular significance, HITECH requires covered entities and their business associates to provide notification in the case of breaches of unsecured PHI. In the event of a breach of unsecured PHI, HITECH requires covered entities to provide notification to affected individuals and to HHS following the discovery of the breach. In some cases, the Act also directs covered entities to provide notification to the media of breaches. In the case of a breach of unsecured PHI at or by a business associate of a covered entity, the Act mandates that the business associate notify the covered entity of the breach. Finally, the Act requires the Secretary of HHS to post on an HHS web site a list of breaches of unsecured PHI involving more than 500 individuals.

A.4 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 that when agencies establish or make changes to a system of records, they must notify the public through a system-of-records notice 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.5 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 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.6 Patient Protection and Affordable Care Act of 2010

Part 1, Section 1561 Recommendations

On March 23, 2010, President Obama signed the Affordable Care Act, which extends health care coverage to an estimated 32 million uninsured individuals and makes coverage more affordable for many others. Section 1561 of the Act requires 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 Committees submitted to the Office of the National Coordinator for Health Information Technology the following approved, initial recommendations, which seek to encourage adoption of modern electronic systems and processes that allow a consumer to seamlessly obtain and maintain the full range of available health coverage and other human services benefits. The core of these recommendations is the belief that the consumer will be best served by a health and human services eligibility and enrollment process that:

- Features a transparent, understandable, and easy-to-use online process that enables consumers to make informed decisions about applying for and managing benefits
- Accommodates the range of user capabilities, languages, and access considerations
- Offers seamless integration between private and public insurance options
- Connects consumers with health coverage as well as other human services such as the Supplemental Nutrition Assistance Program (SNAP) and the Temporary Assistance for Needy Families (TANF) program
- Provides strong privacy and security protections.

Part 2, 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.

Part 3, HHS Final Rule §155.260 Privacy and Security of Personally Identifiable Information

On March 12, 2012, HHS issued the Final Rule on ACA Exchanges, §155.260 Privacy and Security of Personally Identifiable Information. As a condition for processing PII associated with Exchange operations, the Exchanges must establish and implement privacy and security standards addressing these aspects:

- Privacy principles consistent with the HHS Privacy Principles (reference Privacy section of this document)
- Operational, technical, administrative, and physical safeguards that are consistent with applicable laws to ensure the congeniality, integrity, and availability of PII
- Compliance with IRS Code
- Civil penalty for any persons who willingly violate 1411(g) of ACA

A.7 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 agency 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.

Acronyms

ACA	Patient Protection and Affordable Care Act of 2010
CIO	Chief Information Officer
CMS	Centers for Medicare & Medicaid Services
COOP	Continuity of Operations Plan
CP	Certificate Policy
CPS	Certification Practice Statement
CTO	Chief Technology Officer
DCIO	Deputy Chief Information Officer
DHS	Department of Homeland Security
DR	Disaster Recovery
EHR	Electronic Healthcare Records
ERA	Exchange Reference Architecture
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
FTI	Federal Tax Information
HHS	Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act of 1996
HIT	Health Information Technology
HITECH	Health Information Technology for Economic and Clinical Health
ICAM	Identity, Credential, and Access Management
IIHI	Individually Identifiable Health Information
IRS	Internal Revenue Service
IT	Information Technology
MITA	Medicaid Information Technology Architecture
MOU	Memorandum of Agreement
NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency/Internal Report
OCR	Office for Civil Rights
OMB	Office of Management and Budget
ONC	Office of National Coordinator Health Information Technology

PHI	Protected Health Information
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
Pub	Publication
SNAP	Supplemental Nutrition Assistance Program
SP	Special Publication
SSA	Social Security Administration
TANF	Temporary Assistance for Needy Families
VLAN	Virtual Local Area Network

List of References

Cloud Security Alliance. http://www.cloudsecurityalliance.org/

Covered Entity Determination Guide. www.cms.gov/HIPAAGenInfo/06_AreYouaCoveredEntity.asp

e-Government Act of 2002. http://www.whitehouse.gov/omb/memoranda_m03-22

Family Educational Rights and Privacy Act. http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

Federal Identity, Credential and Access Management. http://www.idmanagement.gov/

National Institute of Standards and Technology (NIST), Federal Information Processing Standards (FIPS) Publication (Pub) 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.

NIST, FIPS Pub 200, *Minimum Security Requirements for Federal Information and Information Systems*, May 2006.

NIST, FIPS Pub 140-2, *Security Requirements for Cryptographic Modules*, May 25, 2001.

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

Federal Risk and Authorization Management Program. http://www.cio.gov/pages.cfm/page/Federal-Risk-and-Authorization-Management-Program-FedRAMP

Freedom of Information Act of 1966. http://www.hhs.gov/foia/

Financial Modernization Act of 1999. http://www.ftc.gov/privacy/privacyinitiatives/glbact.html

Health Information Technology for Economic and Clinical Health Act of 2009. http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/hitechenforcementifr.html

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

HIPAA Survival Guide: The HITECH Act and HIPAA. http://www.hipaasurvivalguide.com/hipaa-survival-guide-21.php

HISPC. Privacy and Security Solutions for Interoperable Health Information Exchange Assessment of Variation and Analysis of Solutions. June 30, 2007. http://www.rti.org/pubs/avas.pdf

Medicaid Information Technology Architecture. https://www.cms.gov/MedicaidInfoTechArch/04_MITAFramework.asp

National Association of State Chief Information Officers. *Desperately Seeking Security Frameworks – A Roadmap for State CIOs*, March 2009, http://www.nascio.org/publications/documents/NASCIO-SecurityFrameworks.pdf

NIST, *Guide for Mapping Types of Information and Information Systems to Security Categories*, NIST Special Publication (SP) 800-60, August 2008.

NIST, *An Introduction to Computer Security: The NIST Handbook,* NIST SP 800-12, October 1995.

NIST Cloud Computing Collaboration Site. http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/WebHome

NIST, *Recommended Security Controls for Federal Information Systems Rev 2*, NIST SP 800-53, December 2007.

NIST, *Guide for Assessing the Security Controls in Federal Information Systems*, NIST SP 800-53A, July 2008.

NIST, *Guide for Applying the Risk Management Framework to Federal Information Systems rev1*, NIST SP 800-37, February 2010.

NIST, *An Introductory Resource Guide for Implementing the HIPAA Security Rule*, NIST SP 800-66, Revision 1, October 2008.

NIST, *Exchange Reference Architecture: Foundation Guidance,* Draft*,* Version 0.93, Centers for Medicare & Medicaid Services, February 11, 2011*.*

Office of Management and Budget (OMB), Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information,* May 22, 2007.

Office of the National Coordinator for Health Information Technology: Electronic Eligibility and Enrollment (*Section 1561)* http://healthit.hhs.gov/portal/server.pt?open=512&mode=2&objID=3161

Personally Identifiable Information (PII) Definition. www.whitehouse.gov/sites/omb/memorand/fy2007/m07-16.pdfw

Privacy Act of 1974*.* https://www.cms.gov/PrivacyActof1974/

25 Point Implementation Plan to Reform Federal Information Technology Management, Vivek Kundra*.* U.S. Chief Information Officer, December 9, 2010*.*

Patient Protection and Affordable Care Act, Public Law 111–148, 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

NIST Interagency/Internal Report (NISTIR) 7497, Scholl M, Stine K, Lin K, Steinberg D, *Security Architecture Design Process for Health Information Exchanges (HIEs),* September 30, 2010.

45 CFR Parts 160 and 164, Breach Notification for Unsecured Protected Health Information, Interim Final Rule, August 24, 2009. http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf

Internal Revenue Code 6103*, Confidentiality and Disclosure of Returns and Return Information.* http://www.law.cornell.edu/uscode/26/usc_sec_26_00006103----000-.html

IRS Publication 1075, Tax Information Security Guidelines for Federal, State, and Local Agencies and Entities. http://www.irs.gov/pub/irs-pdf/p1075.pdf

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.