Centers for Medicare & Medicaid Services

MARS-E Document Suite, Version 2.0

Volume I: Harmonized Security and Privacy Framework

Version 2.0

November 10, 2015

Foreword

The Centers for Medicare & Medicaid Services (CMS) has developed, assembled, and implemented a document suite of guidance, requirements, and templates known as the Minimum Acceptable Risk Standards for Exchanges (MARS-E), Version 2.0, in accordance with the agency's Information Security and Privacy programs. The guidance in the MARS-E document suite addresses the mandates of the Patient Protection and Affordable Care Act of 2010 (hereafter simply the "Affordable Care Act" or "ACA"), and Department of Health and Human Services ACA Regulations (45 CFR §§155.260 and 155.280), and applies to all ACA Administering Entities. "Administering Entity" means Exchanges or Marketplaces, whether federal or state, state Medicaid agencies, Children's Health Insurance Program (CHIP) agencies, or state agencies administering the Basic Health Program.

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

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

This *Harmonized Security and Privacy Framework* introduces and defines the CMS framework for managing the security and privacy of the information systems operated by ACA Administering Entities.

CMS intends to foster a collaborative discussion with ACA Administering Entities to ensure that the Harmonized Security and Privacy Framework and the overall Framework solution provide the necessary and effective security and privacy standards for the respective systems and data, as well as a flexible basis to support compliance with applicable federal and state security and privacy laws and regulations.

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

/s/ 11/10/2015

David Nelson Date
Chief Information Officer
Centers for Medicare & Medicaid Services

/s/ 11/10/2015

Emery Csulak Date
Chief Information Security Officer /
Senior Agency Official for Privacy
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 MARS-E document suite, Version 2.0, consisting of:

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

SEEN AND APPROVED:

Internal Revenue Service

Terence V. Milholland Chief Technology Officer (CTO)	/s/ Signature	10/15/2015 Date
Edward T. Killen Director, Privacy Governmental Liaison and Disclosure	/s/ Signature	10/14/2015 Date

Social Security Administration

Marti Eckert Acting Associate Commissioner & Chief Information Security Officer (CISO)	/s/ Signature	09/30/2015 Date

Department of Veterans Affairs

Jim Steele Manager, Health Application Support, Enterprise Application Services 005OP6.2.15, VA OI&T Service Delivery and Engineering	/s/ Signature	11/6/2015 Date

Department of Homeland Security

Mark Schwartz USCIS Chief Information Officer (CIO)	/s/ Signature	10/21/2015 Date
Andrew Onello USCIS Chief Information Security Officer (CISO)	/s/ Signature	10/21/2015 Date

Department of Defense
Defense Manpower Data Center

Mary Snavely-Dixon Director	/s/ Signature	10/19/2015 Date
Kris Hoffman Chief Information Officer (CIO)	/s/ Signature	10/15/2015 Date

Peace Corps

Francisco Reinoso Chief Information Officer (CIO)	/s/ Signature	10/24/2015 Date
Victoria Lowery Director of IT Security Assurance & Compliance	/s/ Signature	10/14/2015 Date

Office of Personnel Management

Donna K. Seymour Chief Information Officer (CIO)	/s/ Signature	10/28/2015 Date
Cord Chase Acting Chief Information Security Officer (CISO)	/s/ Signature	10/28/2015 Date

Executive Summary

This *Harmonized Security and Privacy Framework,* defines a structure for managing the security and privacy requirements of systems deployed to administer the provisions of the Affordable Care Act (ACA) that ensure affordable healthcare for all Americans. The key component of the framework is Volume III of the MARS-E document suite, the *Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges*. The Security and Privacy controls specify applicable policies, standards, and procedures necessary for:

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

The framework is founded upon the ACA, Department of Health and Human Services Regulations implementing the ACA, and Federal Information Security Management Act of 2002, amended by the Federal Information Security Modernization Act of 2014 (FISMA) requirements of the federal government.

Record of Changes

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

CR: Change Request

Table of Contents

List of Figures

List of Tables

1. Introduction

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

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

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

HHS and CMS are responsible for providing guidance and oversight for the Exchanges and the functions they perform as well as the information technology (IT) systems that facilitate eligibility determinations, exemptions, and enrollment in insurance affordability programs. This responsibility includes defining business, information, and technical guidance that will create a common baseline and standards for these IT system implementation activities.

As part of the enrollment process, ACA Administering Entities (AE) must collect PII from applicants for healthcare coverage. For eligibility determination, data matches are made against federal data sources held by various state and federal agencies. Adopting strong security and privacy protections is therefore necessary to meet the regulatory requirements of the program and to establish public trust and confidence that their personal information will be protected.

Federal agencies that provide data for the Exchange program include the Internal Revenue Service (IRS), Social Security Administration (SSA), Department of Defense (DoD), Department of Homeland Security (DHS), Department of Veteran Affairs (VA), Office of Personnel Management (OPM), and Peace Corps. Each agency has unique data protection regulations and requirements. ACA Administering Entities and their contractors must adhere to the data safeguard requirements of the Internal Revenue Code (IRC), 26 U.S.C. §6103 (hereafter simply the "Tax Information Safeguarding Requirements") and all corresponding security

guidance as a condition of receiving Federal Tax Information (FTI). In addition, most, if not all, states also have statutes that protect, in varying degrees, the privacy of PII that is collected or created by a state agency.

Prior to version 1.0 of MARS-E, there was no single, integrated, comprehensive approach to security and privacy that addressed all applicable federal requirements under the Federal Information Security Management Act (FISMA), ACA, and Tax Information Safeguarding Requirements. These laws differ 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 has amended this *Harmonized Security and Privacy Framework* to identify key standards and processes to support compliance with the current body of laws and regulations. Nothing in this document should be construed to eliminate the obligation for an Administering Entity to comply with the requirements of other applicable bodies of laws/regulations that apply to Administering Entities [i.e., Title XVIII and XIX for Medicaid/Children's Health Insurance Program (CHIP) agencies]. Depending on the information processed, an Administering Entity's IT system may be required to meet additional security control requirements as mandated by specific sources, whether federal, state, legal, program, or accounting.

1.1 Purpose and Scope

This *Harmonized Security and Privacy Framework* defines the framework established by the Department for managing the security and privacy of systems deployed to administer the health insurance purchasing aspects of the Affordable Care Act. The scope covers all systems operated by ACA Administering Entities (namely, state Medicaid Agency, state CHIP, state BHP, or an Exchange). The remaining volumes of the MARS-E document suite provide the detailed definition of a common framework of minimum acceptable risk controls that will support collaborative solutions to manage security and privacy risks.

1.2 Audience

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

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

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

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

- Tier 1 – Federal Legislation and Executive Mandates
- Tier 2 – HHS ACA Regulations
- Tier 3 – Federal Regulations and Guidance

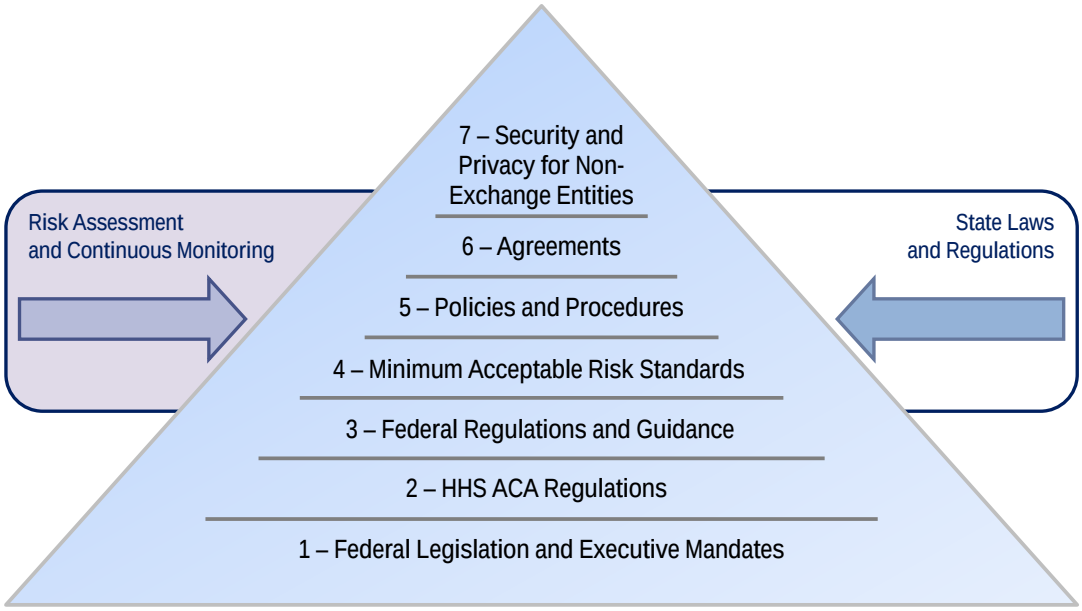

Figure 1. The ACA Security and Privacy Governance Framework

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

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

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

2.1 Tier 1 – Federal Laws and Executive Mandates

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

- Federal Information Security Management Act of 2002, amended by the Federal Information Security Modernization Act of 2014
- Privacy Act of 1974
- e-Government Act of 2002
- Patient Protection and Affordable Care Act of 2010
- HHS ACA Regulation
- Safeguards for Protecting Federal Tax Returns and Return Information (26 U.S.C. §6103 and related provisions)

2.1.1 Determining the Applicability of Federal Mandates

All federal agencies, and in some cases their contractors, must comply with FISMA, the Privacy Act of 1974, and the e-Government Act of 2002. Depending on the types of data created, collected, used, or disclosed, an AE system may need to comply with other federal mandates. Table 1 provides the controlling definitions for four types of data.

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

IRC §6103 applies if an Administering Entity's IT system receives FTI. Federal and non-federal organizations that operate Exchanges must determine their entity classification under HIPAA. Organizations must determine whether they are HIPAA covered entities or business associates. Covered entities are health plans, healthcare clearinghouses, and healthcare providers that transmit PHI electronically in connection with a HIPAA covered transaction. Business associates include persons, entities, or organizations that perform functions or services for or on behalf of HIPAA covered entities that involve the use or disclosure of PHI.

2.2 Tier 2 – HHS ACA Regulations

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

On August 30, 2013, HHS published §155.280– Oversight and monitoring of privacy and security requirements. This regulation provides HHS and Exchanges the authority to perform monitoring and oversight of subject entities. (Appendix A provides a summary of these regulations, and the List of References provides citations to the source material.)

2.3 Tier 3 – Federal Regulations and Guidance

Tiers 3 of the framework comprises the body of IT security and privacy regulations and guidance that form the technical backbone of MARS-E security and privacy control requirements. CMS has adopted the guidance in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, and NIST SP 800-53A Rev 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations* in formulating this release of the security and privacy standards for ACA Administering Entities. Even though state-based AEs need not comply with FISMA, CMS has chosen NIST guidance as the basis for the standards for AEs because it is the *de facto* method for specifying security and privacy control requirements throughout the IT industry.

Furthermore, the privacy control families in NIST SP 800-53 Rev 4 are congruent with the FIPP principles contained in 45 CFR §155.260.

2.4 Tier 4 – Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges

Tier 4, the *Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges* (MARS-E Volume III), is central to the framework. Through this Catalog, CMS identifies the essential set of security and privacy controls that must be adopted by all entities implementing and operating an Exchange and/or Medicaid, CHIP, and Basic Health Program ACA health insurance purchasing systems. CMS established these MARS-E standards based on the agency's interpretation of applicability of Tier 1, Tier 2, and Tier 3 mandates/guidance (as well as the applicability of HHS and CMS internal policies and guidance) to the ACA AE systems

environment. The AEs must implement these controls in conjunction with requirements from other sources mandated for their systems environments.

2.5 Tier 5 – Policies, Guidance, and Procedures

Tier 5 of the framework encompasses the set of policies, guidance, and procedures that support the implementation of required security and privacy controls. CMS has documented agency policies, guidance, and procedures for the technical areas of MARS-E implementation as well as CMS's oversight and monitoring for MARS-E compliance. *Volume II: Minimum Acceptable Risk Standards for Exchanges* provides a full set of references to these documents.

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

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

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

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

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

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

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

entity obtaining access to PII to the security and privacy standards for the use and disclosure of that information.

2.8 Other Considerations

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

Appendix A. Key Laws and Guidance Governing Exchange of PII

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

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

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

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

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

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

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

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

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

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

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

A.2 The Privacy Act of 1974

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

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

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

A.3 The e-Government Act of 2002

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

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

A.4 Patient Protection and Affordable Care Act of 2010

Section 1411(g) Confidentiality of Applicant Information

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

A.5 HHS ACA Regulation

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

Part of the Department of Health and Human Services (HHS) regulation that specifies ACA standards for patient protection is 45 CFR §155.260 – Privacy and security of personally

identifiable information issued on March 12, 2012. (An amendment was issued March 11, 2014). The regulation stipulates that the information collected either directly from an applicant or through other sources can only be used to perform the functions of an Exchange or as the Secretary determines is a function that ensures the efficient operation of the Exchange.

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

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

The detailed contents of §155.260 can be found in Appendix A of V*olume II: Minimum Acceptable Risk Safeguards for Exchanges* of the MARS-E document suite, Version 2.0.

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

45 CFR §155.280 authorized HHS to oversee and monitor the Federally Facilitated Exchange and non-Exchange entities in their compliance with the privacy and security standards established and implemented by a Federally Facilitated Exchange pursuant to §155.260. HHS will also oversee and monitor state Exchanges in their establishment and implementation of privacy and security standards pursuant to §155.260. The state Exchanges have the obligation to oversee and monitor non-Exchange entities in their compliance with privacy and security standards established by the state Exchange pursuant to §155.260.

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

A.6 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.

Master List of Acronyms for MARS-E Document Suite

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

CTO	Chief Technology Officer
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
CWE	Common Weakness Enumeration
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DHS	Department of Homeland Security
DI	Data Quality and Integrity, a Privacy Control family
DISA	Defense Information Systems Agency
DM	Data Minimization and Retention, a Privacy Control family
DMZ	Demilitarized Zone
DNS	Domain Name System
DNSSEC	DNS Security
DoD	Department of Defense
DR	Disaster Recovery, a Security Control family
DSH	CMS Data Services Hub
DTR	Data Testing Report
EAP	Extensible Authentication Protocol
EHR	Electronic Healthcare Record
FDSH	Federal Data Services Hub
FFM	Federally-facilitated Marketplace
FIPPS	Fair Information Protection Principles
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
FOIA	Freedom of Information Act
FTI	Federal Tax Information
FTP	File Transfer Protocol
GAGAS	Generally Accepted Governmental Auditing Standards
GMT	Greenwich Meridian Time
guid	Globally Unique Identifier
HHS	Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act of 1996

HITECH	Health Information Technology for Economic and Clinical Health Act of 2009
HTTP	Hypertext Transfer Protocol
IA	Identification and Authentication, a Privacy Control family
ID	Identity
IDS	Intrusion Detection System
IEA	Information Exchange Agreement
IIHI	Individually Identifiable Health Information
IP	Internet Protocol
IP	Individual Participation and Redress, a Privacy Control family
IPS	Intrusion Prevention System
IR	Incident Response, a Privacy Control family
IRC	Internal Revenue Code
IRS	Internal Revenue Service
IS	Information Security
IS	Information System
ISA	Information Sharing Agreement
ISE	Information Sharing Environment
ISPG	Information Security Privacy Policy and Compliance Group
ISRA	Information Security Risk Assessment
IT	Information Technology
MA	Maintenance, a Security Control family
MAC	Media Access Control
MAGI	Modified Adjusted Gross Income
MARS-E	Minimum Acceptable Risk Standards for Exchanges
MFD	Multi-Function Device
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MP	Media Protection, a Security Control family
MTD	Maximum Tolerable Downtime
NARA	National Archives and Records Administration
NEE	Non-Exchange Entity
NIAP	National Information Assurance Partnership

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

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

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

Master Glossary for MARS-E Document Suite

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

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

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

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

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

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

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

List of References

1. *e-Government Act of 2002*. http://www.whitehouse.gov/omb/memoranda_m03-22
2. Federal Information Security Management Act of 2002, available at: http://csrc.nist.gov/groups/SMA/fisma/index.html
3. Health Insurance Portability and Accountability Act of 1996, available at: http://www.gpo.gov/fdsys/pkg/PLAW-104publ191/content-detail.html
4. 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, available at: http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf
5. NIST, FIPS Pub 200, *Minimum Security Requirements for Federal Information and Information Systems*, May 2006, available at: http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf
6. NIST, Special Publication (SP) 800-53 Rev 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013, available at: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
7. NIST, SP 800-53A Rev 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations*, December 2014, available at: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf
8. Privacy Act of 1974, available at: https://www.cms.gov/PrivacyActof1974/
9. Patient Protection and Affordable Care Act, Public Law 111–148, March 23, 2010, 124 Stat. 119, available at: http://www.gpo.gov/fdsys/pkg/PLAW-111publ148/content-detail.html http://www.healthreform.gov/health_reform_and_hhs.html
10. Department of Health and Human Services Final Rule on Exchange Establishment Standards and Other Related Standards under the Affordable Care Act, 45 CFR Parts 155, 156, and 157, March 12, 2012 as amended, available at: http://www.gpo.gov/fdsys/pkg/FR-2012-03-27/pdf/2012-6125.pdf
11. Amendment(s) to 45 CFR Part 155.260 published March 11, 2014, in 79 FR 13837

    http://www.ecfr.gov/cgi-bin/text-idx?SID=0ff499c497231aa32147d03c31622e81&node=20140311y1.120
12. IRS Publication 1075, *Tax Information Security Guidelines for Federal, State, and Local Agencies and Entities*, available at: http://www.irs.gov/pub/irs-pdf/p1075.pdf
13. NIST, SP 800-66 Revision 1, *An Introductory Resource Guide for Implementing the HIPAA Security Rule*, October 2008, available at: http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf