HIPAA/HITECH: NIST Reference Guideline

NIST References	Description
SP 800-66 Rev. 1 (OIG 2014 Audit)	**An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule** The purpose of this publication is to help educate readers about the security standards included in the HIPAA Security Rule
SP 800-124, Rev.1 (NIST SP 800-66 Rev. 1)	**Guidelines for Managing the Security of Mobile Devices in the Enterprise** This publication provides recommendations for selecting, implementing, and using centralized management technologies, and it explains the security concerns inherent in mobile device use and provides recommendations for securing mobile devices throughout their life cycles
SP 800-115 (NIST SP 800-66 Rev. 1)	**Technical Guide to Information Security Testing** The purpose of this document is to provide guidelines for organizations on planning and conducting technical information security testing and assessments, analyzing findings, and developing mitigation strategies
SP 800-114 (NIST SP 800-66 Rev. 1)	**User's Guide to Securing External Devices for Telework and Remote Access** This publication helps teleworkers secure the external devices they use for telework, such as personally owned and third-party privately owned desktop and laptop computers and consumer devices (e.g., cell phones)
SP 800-113 (NIST SP 800-66 Rev. 1)	**Guide to SSL VPN** This publication seeks to assist organizations in understanding SSL VPN technologies and in designing, implementing, configuring, securing, monitoring, and maintaining SSL VPN solutions
SP 800-111 (NIST SP 800-66 Rev. 1)	**Guide to Storage Encryption Technologies for End User Devices** The purpose of this document is to assist organizations in understanding storage encryption technologies for end user devices and in planning, implementing, and maintaining storage encryption solutions
SP 800-107, Rev. 1 (NIST SP 800-66 Rev. 1)	**Recommendation for Applications Using Approved Hash Algorithms** This document provides security guidelines for achieving the required or desired security strengths when using cryptographic

NIST References	Description
	applications that employ the approved hash functions specified in Federal Information Processing Standard (FIPS) 180-4
SP 800-106 (NIST SP 800-66 Rev. 1)	**Randomized Hashing Digital Signatures** This Recommendation provides a technique to randomize messages that are input to a cryptographic hash function during the generation of digital signatures using the Digital Signature Algorithm (DSA), Elliptic Curve Digital Signature Algorithm (ECDSA) and RSA
SP 800-100 (NIST SP 800-66 Rev. 1)	**Information Security Handbook: A Guide for Managers** The purpose of this publication is to inform members of the information security management team (agency heads; Chief Information Officers [CIOs]; senior agency information security officers [SAISOs], also commonly referred to as Chief Information Security Officers [CISOs]; and Security Managers) about various aspects of information security that they will be expected to implement and oversee in their respective organizations
SP 800-94, Rev. 1 (NIST SP 800-66 Rev. 1)	**Guide to Intrusion Detection and Prevention Systems (IDPS)** This publication seeks to assist organizations in understanding Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) technologies and in designing, implementing, configuring, securing, monitoring, and maintaining Intrusion Detection and Prevention Systems (IDPS)
SP 800-92 (NIST SP 800-66 Rev. 1)	**Guide to Computer Security Log Management** This publication seeks to assist organizations in understanding the need for sound computer security log management
SP 800-88, Rev. 1 (NIST SP 800-66 Rev. 1)	**DRAFT Guidelines for Media Sanitization** This document will assist organizations in implementing a media sanitization program with proper and applicable techniques and controls for sanitization and disposal decisions, considering the security categorization of the associated system's confidentiality
SP 800-86 (NIST SP 800-66 Rev. 1)	**Guide to Integrating Forensic Techniques into Incident Response** This publication is intended to help organizations in investigating computer security incidents and troubleshooting some Information Technology (IT) operational problems by providing practical guidance on performing computer and network forensics
SP 800-84	**Guide to Test, Training, and Exercise Programs for IT Plans**

NIST References	Description
(NIST SP 800-66 Rev. 1)	**and Capabilities** This publication seeks to assist organizations in designing, developing, conducting, and evaluating TT&E events in an effort to aid personnel in preparing for adverse situations involving IT
SP 800-83, Rev. 1 (NIST SP 800-66 Rev. 1)	**Guide to Malware Incident Prevention and Handling** This publication is intended to help a wide variety of organizations understand the threats posed by malware and mitigate the risks associated with malware incidents
SP 800-81-2 (NIST SP 800-66 Rev. 1)	**Secure Domain Name System (DNS) Deployment Guide** This publication seeks to assist organizations in understanding the secure deployment of Domain Name System (DNS) services in an enterprise
SP 800-77 (NIST SP 800-66 Rev. 1)	**Guide to IPsec VPNs** This publication seeks to assist organizations in mitigating the risks associated with the transmission of sensitive information across networks by providing practical guidance on implementing security services based on Internet Protocol Security (IPsec)
SP 800-64, Rev. 2 (NIST SP 800-66 Rev. 1)	**Security Considerations in the Information Systems Development Life Cycle** The purpose of this guideline is to assist agencies in building security into their IT development processes
SP 800-63-1 (OIG 2014 Audit)	**Electronic Authentication Guideline** This recommendation provides technical guidelines to agencies for the implementation of electronic authentication (e-authentication)
SP 800-60, Rev. 1 (NIST SP 800-66 Rev. 1)	**Guide for Mapping Types of Information and Information Systems to Security Categories** This guideline is intended to help agencies consistently map security impact levels to types of: (i) information (e.g., privacy, medical, proprietary, financial, contractor sensitive, trade secret, investigation); and (ii) information systems (e.g., mission critical, mission support, administrative)
SP 800-59 (NIST SP 800-66 Rev. 1)	**Guideline for Identifying an Information System as a National Security System** **This document provides guidelines developed in conjunction with the Department of Defense, including the National Security Agency, for identifying an information**

NIST References	Description
	system as a national security system
SP 800-58 (NIST SP 800-66 Rev. 1)	**Security Considerations for Voice Over IP Systems** The purpose of this document is to provide agencies with guidance for establishing secure VOIP networks
SP 800-55, Rev. 1 (NIST SP 800-66 Rev. 1)	**Performance Measurement Guide for Information Security** This document is a guide for the specific development, selection, and implementation of information system-level and program-level measures to indicate the implementation, efficiency/effectiveness, and impact of security controls, and other security related activities
SP 800-53 Rev. 4 (OIG 2014 Audit)	**Security and Privacy Controls for Federal Information Systems and Organizations** This publication provides a catalog of security and privacy controls for federal information systems and organizations and a process for selecting controls to protect organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation from a diverse set of threats including hostile cyber attacks, natural disasters, structural failures, and human errors (both intentional and unintentional)
SP 800-52, Rev. 1 (NIST SP 800-66 Rev. 1)	**DRAFT Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations** This Special Publication provides guidance to the selection and configuration of TLS protocol implementations while making effective use of Federal Information Processing Standards (FIPS) and NIST recommended cryptographic algorithms
SP 800-50 (NIST SP 800-66 Rev. 1)	**Building an Information Technology Security Awareness and Training Program** This document provides guidelines for building and maintaining a comprehensive awareness and training program, as part of an organization's IT security program
SP 800-48, Rev. 1 (NIST SP 800-66 Rev. 1)	**Guide to Securing Legacy IEEE 802.11 Wireless Networks** The purpose of this document is to provide guidance to organizations in securing their legacy IEEE 802.11 Wireless Local Area Networks (WLAN) that cannot use IEEE 802.11i
SP 800-47 (NIST SP 800-66 Rev. 1)	**Security Guide for Interconnecting Information Technology Systems** This document provides guidance for planning, establishing,

NIST References	Description
	maintaining, and terminating interconnections between Information Technology (IT) systems that are owned and operated by different organizations, including organizations within a single federal agency
SP 800-46 Rev1 (OIG 2014 Audit)	**Guide to Enterprise Telework and Remote Access Security** The purpose of this document is to assist organizations in mitigating the risks associated with the enterprise technologies used for telework, including remote access servers, telework client devices, and remote access communications
SP 800-45, v2 (NIST SP 800-66 Rev. 1)	**Guidelines on Electronic Mail Security** The purpose of the Guidelines on Electronic Mail Security is to recommend security practices for designing, implementing, and operating email systems on public and private networks
SP 800-42 (NIST SP 800-66 Rev. 1)	**Guideline on Network Security Testing** The guide provides an approach for adopting effective procedures that can help organizations uncover unknown vulnerabilities, institute security controls, and prevent incidents and attacks
SP 800-41 (NIST SP 800-66 Rev. 1)	**Guidelines on Firewalls and Firewall Policy** This document provides practical guidance on developing firewall policies and selecting, configuring, testing, deploying, and managing firewalls
SP 800-40 v2 (OIG 2014 Audit)	**Creating a Patch and Vulnerability Management Program** This publication is designed to assist organizations in implementing security patch and vulnerability remediation programs
SP 800-39 (NIST SP 800-66 Rev. 1)	**Managing Information Security Risk: Organization, Mission, and Information System View** The purpose of Special Publication 800-39 is to provide guidance for an integrated, organization-wide program for managing information security risk to organizational operations (i.e., mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation resulting from the operation and use of federal information systems
SP 800-37, Rev. 1 (NIST SP 800-66 Rev. 1)	**Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach**

NIST References	Description
	The purpose of this publication is to provide guidelines for applying the Risk Management Framework to federal information systems to include conducting the activities of security categorization, security control selection and implementation, security control assessment, information system authorization, and security control monitoring
SP 800-35 (NIST SP 800-66 Rev. 1)	**Guide to Information Technology Security Services** The purpose of this guide is to provide assistance with selecting, implementing, and managing IT security services by guiding the organization through the various phases of the IT security services life cycle
SP 800-34 Rev. 1 (OIG 2014 Audit)	**Contingency Planning Guide for Federal Information Systems** This document provides guidelines to individuals responsible for preparing and maintaining Information System Contingency Plans (ISCPs)
SP 800-30 Rev. 1 (NIST SP 800-66 Rev. 1)	**Guide for Conducting Risk Assessments** The purpose of Special Publication 800-30 is to provide guidance for conducting risk assessments of federal information systems and organizations, amplifying the guidance in Special Publication 800-39
SP 800-21 (NIST SP 800-66 Rev. 1)	**Guideline for Implementing Cryptography in the Federal Government** The purpose of this document is to provide guidance to Federal agencies on how to select cryptographic controls for protecting Sensitive Unclassified information
SP 800-18 Rev. 1 (NIST SP 800-66 Rev. 1)	**Guide for Developing Security Plans for Information Technology Systems** The purpose of the system security plan is to provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements
SP 800-16, Rev. 1 (NIST SP 800-66 Rev. 1)	**DRAFT A Role-Based Model for Federal Information Technology / Cyber Security Training** SP 800-16 describes information technology / cyber security role-based training for Federal Departments and Agencies and Organizations (Federal Organizations). Its primary focus is to provide a comprehensive, yet flexible, training methodology for the development of training courses or modules for personnel

NIST References	Description
	who have been identified as having significant information technology / cyber security responsibilities
SP 800-14 (NIST SP 800-66 Rev. 1)	**Generally Accepted Principles and Practices for Securing Information Technology Systems** This document provides a baseline that organizations can use to establish and review their IT security programs
SP 800-12 (NIST SP 800-66 Rev. 1)	**An Introduction to Computer Security: The NIST Handbook** This handbook provides assistance in securing computer-based resources (including hardware, software, and information) by explaining important concepts, cost considerations, and interrelationships of security controls

