SCANNER GRANT

Security Policies Matrix

**Illinois HIE Strategy and Operational Plan**: Security Standards Under the HIPAA Security Rule, a ”covered entity” or “business associate” must comply with specific security standards regarding the confidentiality, integrity, and availability of stored PHI data, precautionary measures regarding reasonably anticipated threats and misuse, and workforce compliance measures. In addition to the security standards, specific rules address administrative safeguards, physical safeguards, technical safeguards, organizational requirements, policies and procedures and documentation requirements. The comprehensive federal standards include security “breach notification” response and reporting obligations. In general, Illinois law does not impose security standards in excess of the federal standards. [www.hie.illinois.gov/assets/hiesop.pdf](http://www.hie.illinois.gov/assets/hiesop.pdf)

**Massachusetts Regulations**: [[MGL c.40J, s.6D](http://www.malegislature.gov/Laws/GeneralLaws/PartI/TitleVII/Chapter40J/Section6D)] Each plan as updated shall: (i) allow seamless, secure electronic exchange of health information among health care providers, health plans and other authorized users; (ii) provide consumers with secure, electronic access to their own health information; (iii) meet all applicable federal and state privacy and security requirements, including requirements imposed by 45 C.F.R. §&sec 160, 162 and 164; (iv) meet standards for interoperability adopted by the institute with the approval of the council; (v) give patients the option of allowing only designated health care providers to disseminate their individually identifiable information; (vi) provide public health reporting capability as required under state law; and (vii) allow reporting of health information other than identifiable patient health information for purposes of such activities as the secretary of health and human services may from time to time consider necessary. [www.malegislature.gov/laws/generallaws/parti/titlevii/chapter40j/section6d](http://www.malegislature.gov/laws/generallaws/parti/titlevii/chapter40j/section6d)

201 CMR 17: (1) Every person that owns or licenses personal information about a resident of the Commonwealth shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to (a) the size, scope and type of business of the person obligated to safeguard the personal information under such comprehensive information security program; (b) the amount of resources available to such person; (c) the amount of stored data; and (d) the need for security and confidentiality of both consumer and employee information. The safeguards contained in such program must be consistent with the safeguards for protection of personal information and information of a similar character set forth in any state or federal regulations by which the person who owns or licenses such information may be regulated. [www.mass.gov/ocabr/docs/idtheft/201cmr1700reg.pdf](http://www.mass.gov/ocabr/docs/idtheft/201cmr1700reg.pdf)

The **California Privacy and Security Advisory Board** developed and approved security requirements for recommendation to the Health and Human Services Agency for adoption. These recommendations in the form of Security Guidelines may be found at [www.ohi.ca.gov](http://www.ohi.ca.gov).

**Tennessee VA** – Under the Information Technology Management Reform Act (Public Law 104-106), the Secretary of Commerce approves standards and guidelines that are developed by the National Institute of Standards and Technology (NIST) for Federal computer systems. These standards and guidelines are issued by NIST as Federal Information Processing Standards (FIPS) for use government-wide. NIST develops FIPS when there are compelling Federal government requirements such as for security and interoperability and there are no acceptable industry standards or solutions. See background information for more details. Since the VA is part of the federal government, they are required to meet the NIST requirements. Special Publication 800-122 Guide for Protecting the Confidentiality of Personally Identifiable Information provides special guidelines for federal agencies that process personally identifiable information. NIST special publications may be found at http://csrc.nist.gov/publications/PubsSPs.html

|  | **facility and equipment Controls** | | |
| --- | --- | --- | --- |
|  | **Illinois and Massachusetts (HIPPA)** | **California (CalPSAB Recommended Requirements)** | **Tennessee VA (NIST)** |
| 1.1 | **Standard: Facility access controls [45 CFR § 164.310(a)(1)]** Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed. | **3 – Facility and Equipment Controls**  **(a) Facility Access Controls**  An entity shall limit physical access to its information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.  *[45 CFR § 164.310 (a)(1)]* | **SP 800-12 An Introduction to Computer Security: The NIST Handbook**  This chapter first discusses basic criteria that can be used to decide whether a particular user should be granted access to a particular system resource. It then reviews the use of these criteria by those who set policy (usually system-specific policy), commonly used technical mechanisms for implementing logical access control, and issues related to administration of access controls.  **800-14 Generally Accepted Principles and Practices for Securing Information Technology Systems**  **3.10 Physical and Environmental Security**  Physical and environmental security controls are implemented to protect the facility housing system resources, the system resources themselves, and the facilities used to support their operation. An organization's physical and environmental security program should address the following seven topics. In doing so, it can help prevent interruptions in computer services, physical damage, unauthorized disclosure of information, loss of control over system integrity, and theft.   * Physical Access Controls * Fire Safety Factors * Failure of Supporting Utilities * Structural Collapse * Plumbing Leaks * Interception of Data * Mobile and Portable Systems   See also SP 800-53 Recommended Security Controls for Federal Information Systems and Organizations.  **FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION (FIPS) 200. Physical and Environmental Protection (PE):** Organizations must: (i) limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; (iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems. |
| 1.2 | No comparable requirement. | **3 – Facility and Equipment Controls**  (a) (2) **Communication & Operations Management** - An entity shall assign responsibilities for the management and operation of all information processing facilities that handle individual health information.  An entity shall establish formal exchange policies, procedures, and controls to protect the exchange of information through the use of all types of communication facilities.  *[ISO/IEC 27002 (17799), Section 10.1 Operational Procedures and Responsibilities,* *10.8 Exchange of Information]* | **SP 800-50 Building an Information Technology Security Awareness and Training Program**  **1.5 Roles and Responsibilities**  While it is important to understand the policies that require agencies to develop and implement awareness and training, it is crucial that agencies understand who has responsibility for IT security awareness and training. This section identifies and describes those within an organization that have responsibility for IT security awareness and training.  Some organizations have a mature IT security program, while other organizations may be struggling to achieve basic staffing, funding, and support. The form that an awareness and training program takes can vary greatly from agency to agency. This is due, in part, to the maturity of that program.3 One way to help ensure that a program matures is to develop and document IT security awareness and training responsibilities for those key positions upon which the success of the program depends.4  **SP 800-100 Information Security Handbook, A Guide for Managers**  **Chapter 2, Information Security Governance**  To ensure an appropriate level of support of agency missions and the proper implementation of current and future information security requirements, each agency should establish a formal information security governance structure.  **2.2.3 Key Governance Roles and Responsibilities**  The Clinger-Cohen Act assigns the responsibility for ensuring “that the information security policies, procedures, and practices of the executive agency are adequate.”  This section includes the duties for the Agency Head, Chief Information Officer, Senior Agency Security Information Officer, Chief Enterprise Architect, and other roles.  See also SP 800-53 Recommended Security Controls for Federal Information Systems and Organizations. |
| 1.3 | **Standard: Device and media controls [45 CFR § 164.310(d)(1)]** Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.  **Federal Register / Vol. 74, No. 79 / Monday, April 27, 2009 Pages** **19006-19010(II)(A) – HITECH Act**  Data comprising PHI can be vulnerable to a breach in any of the commonly recognized data states: ‘‘data in motion’’ (i.e., data that is moving through a network, including wireless transmission – See Preventing Data Leakage Safeguards Technical Assistance, Internal Revenue Service, [http://www.irs.gov/businesses/small/article/0,,id=201295,00.html](http://www.irs.gov/businesses/small/article/0)); ‘‘data at rest’’ (i.e., data that resides in databases, file systems, and other structured storage methods); ‘‘data in use’’ (i.e., data in the process of being created, retrieved, updated, or deleted); or ‘‘data disposed’’ (e.g., discarded paper records or recycled  electronic media). PHI in each of these data states (with the possible exception of ‘‘data in use’’) may be secured using one or more methods. | **3 – Facility and Equipment Controls**  (b) **Device & Media Controls** - An entity shall control, administer and maintain a record of the consignment of hardware and electronic media that contain individual health information and any person responsible therefore and maintain the inventory of such assets. *[45 CFR § 164.310 (d)(1)]*  (b)(2) **Unsecured IHI Loss Prevention** - An entity shall take reasonable steps to prevent the unauthorized removal or transmission of individual health information, including but not limited to, data leakage, laptop or flash drive loss, etc.  *[Federal Register / Vol. 74, No. 79 / Monday, April 27, 2009 Pages* *19006-19010]* | **SP 800-53 Recommended Security Controls for Federal Information Systems and Organizations**, Appendix D  2.2 Security Controls Baseline  To assist organizations in making the appropriate selection of security controls for an information system, the concept of *baseline* controls is introduced. Baseline controls are the starting point for the security control selection process described in this document and are chosen based on the security category and associated impact level of the information system determined in accordance with FIPS 199 and FIPS 200, respectively.  **SP 800-114 User’s Guide to Securing External Devices for Telework and Remote Access**  **AC-17 REMOTE ACCESS**  Control: The organization:   1. Documents allowed methods of remote access to the information system; 2. Establishes usage restrictions and implementation guidance for each allowed remote access method; 3. Monitors for unauthorized remote access to the information system; 4. Authorizes remote access to the information system prior to connection; and 5. Enforces requirements for remote connections to the information system.   Supplemental Guidance: This control requires explicit authorization prior to allowing remote access to an information system without specifying a specific format for that authorization. For example, while the organization may deem it appropriate to use a system interconnection agreement to authorize a given remote access, such agreements are not required by this control. Remote access is any access to an organizational information system by a user (or process acting on behalf of a user) communicating through an external network (e.g., the Internet). Examples of remote access methods include dial-up, broadband, and wireless (see AC-18 for wireless access). A virtual private network when adequately provisioned with appropriate security controls, is considered an internal network (i.e., the organization establishes a network connection between organization- controlled endpoints in a manner that does not require the organization to depend on external networks to protect the confidentiality or integrity of information transmitted across the network). Remote access controls are applicable to information systems other than public web servers or systems specifically designed for public access. Enforcing access restrictions associated with remote connections is accomplished by control AC-3. Related controls: AC-3, AC-18, AC-20, IA-2, IA-3, IA-8, MA-4.  Control Enhancements:   * **(1)  The organization employs automated mechanisms to facilitate the monitoring and control of remote access methods.** Enhancement Supplemental Guidance: Automated monitoring of remote access sessions allows organizations to audit user activities on a variety of information system components (e.g., servers, workstations, notebook/laptop computers) and to ensure compliance with remote access policy. * **(2)  The organization uses cryptography to protect the confidentiality and integrity of remote access sessions.**  Enhancement Supplemental Guidance: The encryption strength of mechanism is selected based on the security categorization of the information. Related controls: SC-8, SC-9, SC-13. * **(3)  The information system routes all remote accesses through a limited number of managed access control points.**  Enhancement Supplemental Guidance: Relatedcontrol:SC-7. * **(4)  The organization authorizes the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs and documents the rationale for such access in the security plan for the information system.**  Enhancement Supplemental Guidance: Relatedcontrol:AC-6. * **(5)  The organization monitors for unauthorized remote connections to the information system [Assignment: *organization-defined frequency],* and takes appropriate action if an unauthorized connection is discovered.** * **(6)  The organization ensures that users protect information about remote access mechanisms from unauthorized use and disclosure.** * **(7)  The organization ensures that remote sessions for accessing [Assignment: *organization-defined list of security functions and security-relevant information]* employ [Assignment: *organization- defined additional security measures]* and are audited.**  Enhancement Supplemental Guidance: Additional security measures are typically above and beyond standard bulk or session layer encryption (e.g., Secure Shell [SSH], Virtual Private Networking [VPN] with blocking mode enabled). Related controls: SC-8, SC-9. * **(8)  The organization disables [Assignment: *organization-defined networking protocols within the information system deemed to be nonsecure]* except for explicitly identified components in support of specific operational requirements.**  Enhancement Supplemental Guidance: The organization can either make a determination of the relative security of the networking protocol or base the security decision on the assessment of other entities. Bluetooth and peer-to-peer networking are examples of less than secure networking protocols.   **FIPS 200.** **Media Protection (MP):** Organizations must: (i) protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse.  **System and Communications Protection (SC):** Organizations must:(i) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems. |
| 1.4 | **Standard: Workstation security [45 CFR § 164.310(c)]**  Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users. | **3 – Facility and Equipment Controls**  (b)(3) **Workstation & Security Equipment Controls** - An entity shall implement physical and/or technical safeguards for all workstations that access individual health information, to restrict access to authorized users.  *[45 CFR § 164.310 (c)]* | **SP 800-12 An Introduction to Computer Security: The NIST Handbook**  14.5.4 Physical Access Protection  Media can be stolen, destroyed, replaced with a look-alike copy, or lost. Physical access controls, which can limit these problems, include locked doors, desks, file cabinets, or safes.  If the media requires protection at all times, it may be necessary to actually output data to the media in a secure location (e.g., printing to a printer in a locked room instead of to a general- purpose printer in a common area).  See also SP 800-88 Guide for Media Sanitation and  SP 800-53 Recommended Security Controls for Federal Information Systems and Organizations. |
| 1.5 | **Media re-use (Required) [45 CFR § 164.310(d)(2)(ii)]** Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use. | **3 – Facility and Equipment Controls**  (b)(4) **Reuse of Media** - An entity shall implement procedures for removal of individual health information from electronic media before the media is made available for re-use.  *[45 CFR § 164.310 (d)(2)(ii)]* | **SP 800-111 Guide to Storage Encryption Technology for End User Devices**  **Executive Summary**  Many threats against end user devices could cause information stored on the devices to be accessed by unauthorized parties. To prevent such disclosures of information, particularly of personally identifiable information (PII) and other sensitive data, the information needs to be secured. Securing other components of end user devices, such as operating systems, is also necessary, but in many cases additional measures are needed to secure the stored information.  The primary security controls for restricting access to sensitive information stored on end user devices are encryption and authentication.  **SP 800-88 Guide for Media Sanitation**  Executive Summary  This guide will assist organizations and system owners in making practical sanitization decisions based on the level of confidentiality of their information.  See also SP 800-53 Recommended Security Controls for Federal Information Systems and Organizations. |
| 1.6 | **Disposal (Required) [45 CFR § 164.310(d)(2)(i)]**  Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.  **Reference Citation: (HITECH) Federal Register / Vol. 74, No. 79 / Monday, April 27, 2009 Pages 19006-19010(II)(B)**  (b) The media on which the PHI is stored or recorded has been destroyed in one of the following ways:  (i) Paper, film, or other hard copy media have been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed.  (ii) Electronic media have been cleared, purged, or destroyed consistent with *NIST Special Publication 800–88, Guidelines for Media Sanitization*, such that the PHI cannot be retrieved. | **3 – Facility and Equipment Controls**  (b)(5) **Disposal of Media** - An entity shall utilize a method that best meets the entity’s business practices and protects the security of individual health information for final disposition of individual health information, hardware, and/or electronic media on which the individual health information is stored.  The media on which the IHI is stored or recorded shall be destroyed in one of the following ways:   * Paper, film, or other hard copy media have been shredded or destroyed such that the IHI cannot be read or reconstructed. Redaction is specifically excluded as a means of data destruction. * Electronic media have been cleared, purged, or destroyed consistent with NIST Special Publication 800–88, Guidelines for Media Sanitization.   *[45 CFR § 164.310 (d)(2)(i), Federal Register / Vol. 74, No. 79 / Monday, April 27, 2009 Pages* *19006-19010]* | **SP 800–88 Guidelines for Media Sanitization**  **2.1 Need for Proper Media Sanitization and Information Disposition**  Media sanitization is one key element in assuring confidentiality. Confidentiality is “Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information...” [44 U.S.C., Sec. 3542]  “A loss of confidentiality is the unauthorized disclosure of information.” [FIPS-199, Standards for Security Categorization of Federal Information and Information Systems]  In order for organizations to have appropriate controls on the information they are responsible for safeguarding, they must properly safeguard used media. An often rich source of illicit information collection is either through dumpster diving for improperly disposed hard copy media, acquisition of improperly sanitized electronic media, or through keyboard and laboratory reconstruction of media sanitized in a manner not commensurate with the confidentiality of its information. Media flows in and out of organizational control through recycle bins in paper form, out to vendors for equipment repairs, and hot swapped into other systems in response to emergencies. This potential vulnerability can be mitigated through proper understanding of where information is location, what that information is and how to protect it.  See also SP 800-53 Recommended Security Controls for Federal Information Systems and Organizations. |
| 1.7 | **General requirements [45 CFR § 164.306(a)(1)]**  Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits. | **3 – Facility and Equipment Controls**  (c) **Technical Controls** - An entity shall protect individual health information in information systems as specified in the guidelines.  *[45 CFR § 164.312]* | **SP 800-122 Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)**   1. Obligations to Protect Confidentiality. An organization that is subject to any obligations to protect PII should consider such obligations when determining the PII confidentiality impact level. Obligations to protect generally include laws, regulations, or other mandates (e.g., Privacy Act, OMB guidance). For example, some Federal agencies, such as the Census Bureau and the Internal Revenue Service (IRS), are subject to specific legal obligations to protect certain types of PII.10   See also SP 800-53 Recommended Security Controls for Federal Information Systems and Organizations.  **FIPS 200**. **System and Information Integrity (SI):** Organizations must: (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response. |
| 1.8 | **Log-in monitoring (Addressable) [45 CFR § 164.308(a)(5)(ii)(C)]** [Implement] Procedures for monitoring log-in attempts and reporting discrepancies. | **3 – Facility and Equipment Controls**  (c)(1) **Login Monitoring** - An entity shall monitor log-in attempts, reporting discrepancies, and take actions to remediate, as appropriate.  *[45 CFR § 164.308 (a)(5)(ii)(C)]* | **SP 800-66 An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule**  This Special Publication summarizes the HIPAA security standards and explains some of the structure and organization of the Security Rule. The publication helps to educate readers about information security terms used in the HIPAA Security Rule and to improve understanding of the meaning of the security standards set out in the Security Rule.  **SP 800-53 Recommended Security Controls for Federal Information Systems and Organizations**  **AC-6 LEAST PRIVILEGE**  Control: The organization employs the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.  Supplemental Guidance: The access authorizations defined in this control are largely implemented by control AC-3. The organization employs the concept of least privilege for specific duties and information systems (including specific ports, protocols, and services) in accordance with risk assessments as necessary to adequately mitigate risk to organizational operations and assets, individuals, other organizations, and the Nation. Related controls: AC-2, AC-3, CM-7.  Control Enhancements:  **The organization explicitly authorizes access to [Assignment: *organization-defined list of security functions (deployed in hardware, software, and firmware) and security-relevant information].***  Enhancement Supplemental Guidance: Establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters are examples of security functions. Explicitly authorized personnel include, for example, security administrators, system and network administrators, system security officers, system maintenance personnel, system programmers, and other privileged users. Related control: AC-17.  **The organization requires that users of information system accounts, or roles, with access to [Assignment: *organization-defined list of security functions or security-relevant information],* use non-privileged accounts, or roles, when accessing other system functions, and if feasible, audits any use of privileged accounts, or roles, for such functions.**  Enhancement Supplemental Guidance: This control enhancement is intended to limit exposure due to operating from within a privileged account or role. The inclusion of *role* is intended to address those situations where an access control policy such as *Role Based Access Control (RBAC)* is being implemented and where a change of role provides the same degree of assurance in the change of access authorizations for both the user and all processes acting on behalf of the user as would be provided by a change between a privileged and non-privileged account. Audit of privileged activity may require physical separation employing information systems on which the user does not have privileged access.  **The organization authorizes network access to [Assignment: *organization-defined privileged commands]* only for compelling operational needs and documents the rationale for such access in the security plan for the information system.**  **The information system provides separate processing domains to enable finer-grained allocation of user privileges.**  APPENDIX F-AC  PAGE F-9  Special Publication 800-53 Recommended Security Controls for Federal Information Systems and Organizations  Enhancement Supplemental Guidance: Employing virtualization techniques to allow greater privilege within a virtual machine while restricting privilege to the underlying actual machine is an example of providing separate processing domains for finer-grained allocation of user privileges.   1. **The organization limits authorization to super user accounts on the information system to designated system administration personnel.**  Enhancement Supplemental Guidance: Super user accounts are typically described as “root” or “administrator” for various types of commercial off-the-shelf operating systems. Configuring organizational information systems (e.g., notebook/laptop computers, servers, workstations) such that day-to-day users are not authorized access to super user accounts is an example of limiting system authorization. The organization may differentiate in the application of this control enhancement between allowed privileges for local information system accounts and for domain accounts provided the organization retains the ability to control the configuration of the system with regard to key security parameters and as otherwise necessary to sufficiently mitigate risk. 2. **The organization prohibits privileged access to the information system by non-organizational users.  Enhancement Supplemental Guidance: A qualified organizational user may be advised by an organizational user, if necessary.**   See also SP 800-53 Recommended Security Controls for Federal Information Systems and Organizations and  SP 800-100 Information Security Handbook: A Guide for Managers  **FIPS 200**. **Access Control (AC):** Organizations must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise. |
| 1.9 | No comparable requirement. | **3 – Facility and Equipment Controls**  (c)(4) **Email & Messaging Security** - An entity shall safeguard electronic mail and messaging containing individual health information in its possession.  *[ISO/IEC 27002 (17799) 10.8.4 Electronic* *Messaging]* | 1. **SP 800-45 V2 Guidelines on Electronic Mail Security** 2. This document is intended to assist organizations in installing, configuring, and maintaining secure mail servers and mail clients. More specifically, this document discusses the following items in detail:    * Email standards and their security implications    * Email message signing and encryption standards    * Planning and management of mail servers    * Securing the operating system underlying a mail server    * Mail server application security    * Email content filtering    * Email-specific considerations in the deployment and configuration of network protection mechanisms, such as firewalls, routers, switches, and intrusion detection and intrusion prevention systems    * Securing mail clients    * Administering the mail server in a secure manner, including backups, security testing, and log  reviews.   See SP 800-45 Recommended Security Controls for Federal Information Systems and Organizations for specific standards for email.  **FIPS 200.** **System and Communications Protection (SC):** Organizations must:(i) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems. |
| 1.10 | **Standard: Audit controls [45 CFR § 164.312(b)]**  Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information. | **3 – Facility and Equipment Controls**  (c)(5) **Audit Controls** - An entity shall implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use individual health information.  *[45 CFR* *§ 164.312(b)]* | **SP 800-92 Guide to Computer Security Log Management**  **Chapter 18**  Audit trails maintain a record of system activity both by system and application processes and by user activity of systems and applications. In conjunction with appropriate tools and procedures, audit trails can assist in detecting security violations, performance problems, and flaws in applications.  See also SP 800-53 Recommended Security Controls for Federal Information Systems and Organizations.  FIPS 200. **Audit and Accountability (AU):** Organizations must: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions. |
| 1.11 | No comparable requirement. | **3 – Facility and Equipment Controls**  (d) **Network Security Management** - An entity shall protect the networks and infrastructures that maintain or transmit individual health information.  *[ISO/IEC 27002 (17799) 10.6 Network Security*  *Management]* | Standards for network security management may be found in the following special publications.  **SP 800-153 Draft Guideline for Securing Wireless Local Area Networks**  Organizations should implement the following guidelines to improve the security of their WLANs.   * Have standardized security configurations for common WLAN components, such as client devices and APs. * When planning WLAN security, consider the security not only of the WLAN itself, but also how it may affect the security of other networks. * Have policies that clearly state which forms of dual connections are permitted or prohibited for WLAN client devices, and enforce these policies through the appropriate security controls. * Ensure that the organization’s WLAN client devices and APs have configurations at all times that are compliant with the organization’s WLAN policies. * Perform both attack monitoring and vulnerability monitoring to support WLAN security. * Conduct regular periodic technical security assessments for the organization’s WLANs.   **SP 800-44** **Guidelines on Security Public Web Servers**  Organizations should implement appropriate security management practices and controls when maintaining and operating a secure Web server.  **SP 800-127 Guide to Securing WiMAX Wireless Communications**  Organizations should develop a robust WMAN security policy and enforce it.  **SP 800-120 Recommendations for EAP Methods Used in Wireless Network Access Authentication**  This Recommendation formalizes a set of core security requirements for EAP methods when employed by the U.S. Federal Government for wireless access authentication and key establishment. The requirements **should** be considered as generic, in the sense that they are independent of specific wireless technologies. When there are differences between this Recommendation and the referenced IEEE and IETF standards, this Recommendation **shall** have precedence for U.S. Government applications. This Recommendation addresses the validation of a few selected EAP methods, in order to explain the requirements. |
| 1.12 | No comparable requirement. | **3 – Facility and Equipment Controls**  (d)(1) **Perimeter Controls & Management** - An entity shall identify and include, or reference, security features, service levels, and management requirements of all network services in any network services agreement, whether these services are provided in-house or outsourced. Network services include the provision of connections, private network services, and value added networks and managed network security solutions such as firewalls and a system to detect intrusion.  *[ISO/IEC 27002 (17799) 10.6.2 Security of Network Services]* | **SP 800-47 Security Guide for Interconnecting Information Technology Systems**  3.5 Step 5: Document Interconnection Agreement  The joint planning team should document an agreement governing the interconnection and the terms under which the organizations will abide by the agreement, based on the team’s review of all relevant technical, security, and administrative issues (Section 3.4 above). Two documents may be developed: an ISA and an MOU/A. These documents are discussed below.4  A sample Agreement is in Appendix A of this SP. |
| 1.13 | No comparable requirement. | **3 – Facility and Equipment Controls**  (d)(2) **Intrusion Detection** - An entity shall implement an internal system to detect intrusion attempts. The entity shall document and report successful intrusions to the primary security official or designee for response.  *[NIST SP 800-94 Guide to Intrusion Detection and Prevention Systems (IDPS)]* | **NIST SP 800-94 Guide to Intrusion Detection and Prevention** **Systems (IDPS)**  Executive Summary – Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices. Intrusion prevention is the process of performing intrusion detection and attempting to stop detected possible incidents. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, attempting to stop them, and reporting them to security administrators. In addition, organizations use IDPSs for other purposes, such as identifying problems with security policies, documenting existing threats, and deterring individuals from violating security policies. IDPSs have become a necessary addition to the security infrastructure of nearly every organization. |
| 1.14 | **Standard: Access Control [45 CFR § 164.312(a)(1)]**  Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in *45 CFR § 164.308(a)(4).* | **4 – Data Protection and User Access Control**  (a) **Access Controls** - An entity shall utilize identity management, authentication, and authorization mechanisms to ensure that only authorized users have access to information systems.  *[45 CFR § 164.312 (a)(1)]* | **SP 800-53 Recommended Security Controls For Federal Information Systems and Organizations**  **APPENDIX F SECURITY CONTROL CATALOG**  SECURITY CONTROLS, ENHANCEMENTS, AND SUPPLEMENTAL GUIDANCE  The catalog of security controls in this appendix provides a range of safeguards and countermeasures for organizations and information systems. The organization of the security control catalog, the structure of the controls, and the concept of allocating security controls and control enhancements to the initial baselines in Appendix D are described in Chapter Two. The security controls in the catalog are expected to change over time, as controls are withdrawn, revised and added. In order to maintain stability in security plans and automated tools supporting the implementation of NIST Special Publication 800-53, security controls and control enhancements will not be renumbered each time a control or enhancement is withdrawn. Notations of security controls and controls enhancements that have been withdrawn will be maintained in the catalog for historical purposes  **SP 800-63** **Electronic Authentication Guidelines**  This recommendation provides technical guidelines for Federal agencies implementing electronic authentication, and it is not intended to constrict the development or use of standards outside of this purpose. The recommendation covers remote authentication of users over open networks. It defines technical requirements for each of four levels of assurance in the areas of identity proofing, registration, tokens, management processes, authentication protocols and related assertions.  **FIPS 200. Access Control (AC):** Organizations must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise. |

|  | **DATA PROTECTION AND USER ACCESS Controls** | | |
| --- | --- | --- | --- |
|  | **Illinois and Massachusetts (HIPPA)** | **California (CalPSAB Recommended Requirements)** | **Tennessee VA (NIST)** |
| 2.1 | **Standard: Verification Requirements [45 CFR § 164.514(h)(1)(ii)]**  (h)(1) Standard: Verification requirements. Prior to any disclosure permitted by this subpart, a covered entity must:  (ii) Obtain any documentation, statements, or representations, whether oral or written, from the person requesting the protected health information when such documentation, statement, or representation is a condition of the disclosure under this subpart. | **4 – Data Protection and User Access Control**  (a)(1) **Identity Management (Internal)**  An entity shall establish policies and procedures to verify the identity of workforce members who will access the entity’s systems. An entity shall, at a minimum:   Verify that the individual is the one claimed by examination of various forms of state-issued picture identifications such as a driver’s license or ID card, professional licenses in good standing from state or national certification boards, and other forms of identification issued by reliable bodies. The number and extent of such verification will be commensurate with the user’s responsibilities and consistent with privileges they will be given (authorizations). | **NIST SP 800-63 (Section 7) Requirements per Assurance Level**  At Level 2 and higher, records of registration shall be maintained either by the RA or by the CSP, depending on the context. Either the RA or the  CSP shall maintain a record of each individual whose identity has been verified, and the steps taken to verify his or her identity, including the evidence required in the sections below. The CSP shall be prepared to provide records of identity proofing to Relying Parties as necessary. The identity proofing and registration process shall be performed according to a written policy or practice statement that specifies the particular steps taken to verify identities.  **FIPS 200. Identification and Authentication (IA):** Organizations must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems. |
| 2.2 | **Standard: Person or Entity Authentication [45 CFR *§* 164.312(d)]** Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed. | * Issue a user identifier and an identity certificate and/or token (password, hard token, soft cryptographic token or one-time password device tokens, etc.), appropriate to their level of authorization. | **SP 800-103 An Ontology of Identity Credentials**  1.3 Purpose  This two-part report describes an ontology of identity credentials, explicitly represented as Extensible Markup Language (XML) schemas, as a framework for retention and exchange of identity credential information.  The primary motivation of this work is to support the requirements of identity credential issuers (e.g., issuers of identity cards, passports, and driver licenses) to manage information about supporting documents and issued credentials.  Supporting documents are of many types and origins. They may be issued by United States (U.S.) national parties, or by international parties. Today, they are usually printed or written documents, and in some cases, the only evidence of issuance may be the hardcopy document itself.  The ontology therefore provides a bridge to the future, a means to represent both identity document content and metadata (i.e., descriptive information) in a standard, electronic form to facilitate automation of identity management systems.  An ontology of identity credentials can be used in many ways. It may be used to:   * Produce faithful electronic copies of presented identity credentials and documents for archival storage and exchange, * Create electronic replica credentials from hardcopy source credentials, and, * Create abstracts of electronic credentials that are easy to share and reuse.  A domain ontology can serve these roles because it is more than a data model. An ontology describes the relationships among actors, actions, and objects, and in by so doing, establishes a theory in which all use cases may be expressed.   See also SP 800-53 Recommended Security Controls for Federal Information Systems and Organizations.  **FIPS 200. Identification and Authentication (IA):** Organizations must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems. |
| 2.3 | **Unique user identification (Required) [45 CFR *§* 164.312(a)(2)(i)]** Assign a unique name and/or number for identifying and tracking user identity. | * Be responsible for any health data access rights assigned to the authorized person based on their qualifications and roles. | **SP 800-63 Electronic Authentication Guidelines**  **5. E-Authentication Model**  E-authentication begins with *registration.* An *applicant* applies to a *Registration Authority (RA)* to become a *subscriber* of a *Credential Service Provider (CSP)* and, as a subscriber, is issued or registers a secret, called a *token,* and a *credential* that binds the token to a name and possibly other attributes that the RA has verified. The token and credential may be used in subsequent authentication events.  See also: SP 800-78 Cryptographic Algorithms and Key Sizes for Personal Identity Verification and  See also SP 800-53 Recommended Security Controls for Federal Information Systems and Organizations. |
| 2.4 | **Access establishment and modification (Addressable) [45 CFR *§*** **164.308(a)(4)(ii)(C)]**  Implement policies and procedures that, based upon the entity’s access authorization policies, establish, document, review, and modify a user’s right of access to a workstation, transaction, program, or process. | * Manage all stages in the life- cycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access to information systems and services.   *[45 CFR §§§§ 164.514(h)(1)(ii),* *164.312(d), 164.312(a)(2)(i),* *164.308(a)(4)(ii)(C), NIST SP 800-* *63 (Section 6.3.1) Requirements per Assurance Level, ISO/IEC 27002 (17799) 11.2* *User Access Management]* | **NIST SP 800-63 (Section 7) Requirements per Assurance Level**  At Level 2 and higher, records of registration shall be maintained either by the RA or by the CSP, depending on the context. Either the RA or the  CSP shall maintain a record of each individual whose identity has been verified, and the steps taken to verify his or her identity, including the evidence required in the sections below. The CSP shall be prepared to provide records of identity proofing to Relying Parties as necessary. The identity proofing and registration process shall be performed according to a written policy or practice statement that specifies the particular steps taken to verify identities.  See also SP 800-53 Recommended Security Controls for Federal Information Systems and Organizations. |
| 2.5 | **Unique user identification (Required) [45 CFR *§* 164.312(a)(2)(i)]** Assign a unique name and/or number for identifying and tracking user identity.  164.312 Technical safeguards.  A covered entity must, in accordance with 164.306:  (a)(1) Standard: Access Control. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in section 164.308(a)(4).  See next section. | **4 – Data Protection and User Access Control**  (a)(2) **Single Entity Authentication (Non-Federated)**  An entity shall authenticate each authorized user’s identity prior to providing access to individual health information.  An entity shall assign a unique name and/or number for identifying and tracking user identity and implement procedures to verify that a person or entity seeking access to individual health information is the one claimed.  An entity shall authenticate each user to access that complies with the entity’s level of trust agreement with the external exchange entity.  An entity shall authenticate users attempting to access individually identifiable health information from an unsecured location or device, shall require NIST Level 3 authentication in which the data requester must establish two factors of authentication.  *NIST SP 800-63 Rev-1,* *45 CFR §§ 164.312 (a)(2)(i) &* *164.312 (d), NIST SP 800-63 Rev 1* *Electronic Authentication Guideline, OMB Safeguarding Against and Responding to the Breach of Personally Identifiable Information* *M 07-16]* | **NIST SP 800-63 Rev 1 Electronic Authentication Guideline**  *3-Introduction* – Electronic authentication (E-authentication) is the process of establishing confidence in user identities electronically presented to an information system. E-authentication presents a technical challenge when this process involves the remote authentication of individual guidelines to agencies to allow an individual person to remotely authenticate his/her identity to a Federal IT system. This recommendation also provides guidelines for Verifiers, Relying Parties and Credential Service Providers.  These technical guidelines supplement *OMB guidance, E-Authentication Guidance for Federal Agencies, [OMB M-04-04]* that defines four levels of assurance Levels 1 to 4, in terms of the consequences of the authentication errors and misuse of credentials. Level 1 is the lowest assurance level and Level 4 is the highest. The guidance defines the required level of authentication assurance in terms of the likely consequences of an authentication error. As the consequences of an authentication error become more serious, the required level of assurance increases. The OMB guidance provides agencies with criteria for determining the level of E-authentication assurance required for specific electronic transactions and systems, based on the risks and their likelihood of occurrence.  See also SP 800-53 Recommended Security Controls for Federal Information Systems and Organizations. |
| 2.6 | **Access establishment and modification (Addressable) [45 CFR *§*** **164.308(a)(4)(ii)(C)]**  Implement policies and procedures that, based upon the entity’s access authorization policies, establish, document, review, and modify a user’s right of access to a workstation, transaction, program, or process. | See immediately above. | **SP 800-102 The Ontology of Identity Credentials**  This two-part report describes an ontology of identity credentials, explicitly represented as Extensible Markup Language (XML) schemas, as a framework for retention and exchange of identity credential information. The primary motivation of this work is to support the requirements of identity credential issuers (e.g., issuers of identity cards, passports, and driver licenses) to manage information about supporting documents and issued credentials. Supporting documents are of many types and origins. They may be issued by United States (U.S.) national parties, or by international parties. Today, they are usually printed or written documents, and in some cases, the only evidence of issuance may be the hardcopy document itself. The ontology therefore provides a bridge to the future, a means to represent both identity document content and metadata (i.e., descriptive information) in a standard, electronic form to facilitate automation of identity management systems.  See also SP 800-53 Recommended Security Controls for Federal Information Systems and Organizations. |
| 2.7 | No comparable requirement. | **4 – Data Protection and User Access Control**  **(a)(3) Authentication Across Multiple Entities (Federated)**  If an entity is participating in a trust network HIE:   * The trust network shall manage entity authentication for those participating on the trust network, and * An entity shall manage user authentication only for those entities participating on the trust network.   If the user authentication process is across multiple systems or entities, an entity shall implement the agreed upon authentication process among the participants in the trust network.  An entity participating in the trust network shall implement a trust agreement.  *For example, an entity may use an Interconnections Security Agreement (ISA) and Memorandum of Understanding (MOU) in accordance with NIST SP 800-47 Federal Security Guide for Interconnecting Information Technology Systems (Appendix B), unless such requirement has been superseded by implementation of the national Data Use and Reciprocal Support Agreement (DURSA).* | **NIST SP 800-47 Federal Security Guide for Interconnecting Information Technology Systems**  The Security Guide for Interconnecting Information Technology Systems provides guidance for planning, establishing, maintaining, and terminating interconnections between information technology (IT) systems that are owned and operated by different organizations.  Appendix A Interconnection Security Agreement  The organizations that own and operate the connected information technology (IT) systems should develop an Interconnection Security Agreement (ISA) (or an equivalent document) to document the technical requirements of the interconnection.  A sample agreement is provided in this Appendix. |
| 2.8 | No comparable requirement. | **4 – Data Protection and User Access Control**  (a)(4) **Authorization & Access Control**  An entity shall use the following access control attributes to determine if a user is authorized to access requested information in a way that corresponds to, and is compliant with, the data use agreements governing such access and as it aligns with state requirements:   * Data Source; * Entity of Requestor; * Role of Requestor; * Use of Data; * Sensitivity of Data; * Consent Directives of the Data Subject   An entity that acts as a data requestor shall execute the authorization process at the location agreed upon in the data use agreements governing that exchange. The data requestor shall pass the authentication and authorization to the data supplier as a single message if so designated by the data use agreement.  *[CalPSAB Security Guidelines, Section 4(a)(4)]* | **SP 800-53 Recommended Security Controls For Federal Information Systems and Organizations**  **APPENDIX F SECURITY CONTROL CATALOG**  SECURITY CONTROLS, ENHANCEMENTS, AND SUPPLEMENTAL GUIDANCE  The catalog of security controls in this appendix provides a range of safeguards and countermeasures for organizations and information systems. The organization of the security control catalog, the structure of the controls, and the concept of allocating security controls and control enhancements to the initial baselines in Appendix D are described in Chapter Two. The security controls in the catalog are expected to change over time, as controls are withdrawn, revised and added. In order to maintain stability in security plans and automated tools supporting the implementation of NIST Special Publication 800-53, security controls and control enhancements will not be renumbered each time a control or enhancement is withdrawn. Notations of security controls and controls enhancements that have been withdrawn will be maintained in the catalog for historical purposes |
| 2.9 | **Password management (Addressable) [45 CFR *§* 164.308(a)(5)(ii)(D)]** [Implement] Procedures for creating, changing, and safeguarding passwords. | **4 – Data Protection and User Access Control**  (a)(5) **Password Management**  Where an entity uses password authentication, it shall require passwords to be created, changed periodically, safeguarded, and of sufficient length and complexity to protect individual health information.  *Note*: As applicable, passwords shall be used for all mobile computing devices and passive storage media that contain IHI.  *[45 CFR § 164.308 (a)(5)(ii)(D)]* | **SP 800-73 Interfaces for Personal Identity Verification** (4 Parts)  SP 800-63 Authentication  *5.2 Tokens*  Authentication systems are often categorized by the number of factors that they incorporate. The three factors often considered as the cornerstone of authentication are:   * 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 voice print or other biometric)   *8.2.2.4.Password Strength*  For password based Level 2 authentication systems, the probability of success of an on- line password guessing attack by an attacker who has no *a priori* knowledge of the password, but knows the user name of the target, shall not exceed 2-14 (1 in 16,384), over the life of the password. Level 2 passwords shall have at least 10 bits of min-entropy. Appendix A contains information about estimating the entropy of passwords.  **SP 800-118** **DRAFT Guide to Enterprise Password Management**  NIST announces that Draft Special Publication (SP) 800-118, *Guide to Enterprise Password Management*, has been released for public comment. SP 800-118 is intended to help organizations understand and mitigate common threats against their character-based passwords. The guide focuses on topics such as defining password policy requirements and selecting centralized and local password management solutions.  See also 800-53 Recommended Security Controls for Federal Information Systems and Organizations. |
| 2.10 | **Standard: Integrity [45 CFR *§* 164.312(c)(1)]**  Implement policies and procedures to protect electronic protected health information from improper alteration or destruction. | **4 – Data Protection and User Access Control**  (b) **Data Assurance**  An entity shall protect individual health information from unauthorized alteration or destruction.  An entity shall implement technical security measures to guard against unauthorized access to, or modification of, individual health information that is being transmitted over an electronic communications network.  *[45 CFR §§ 164.312 (c)(1) &* *164.312 (e)(1)]* | **SP 800-53 Recommended Security Controls for Federal Information Systems and Organizations**  Appendix F-SC  **SC-21 SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)**  Control: The information system performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources when requested by client systems.  See also:  SP 800 SP 800-47 Security Guide for Interconnecting Information Technology Systems  SP 800-63 Electronic Authentication Guidelines  **FIPS 200**. **System and Information Integrity (SI):** Organizations must: (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response. |
| 2.11 | **Standard: Transmission Security [45 CFR § 164.312(e)(1)]** Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. | See immediately above. | Standards for network security management may be found in the following special publications.  **SP 800-153 Draft Guideline for Securing Wireless Local Area Networks**  Organizations should implement the following guidelines to improve the security of their WLANs.   * Have standardized security configurations for common WLAN components, such as client devices and APs. * When planning WLAN security, consider the security not only of the WLAN itself, but also how it may affect the security of other networks. * Have policies that clearly state which forms of dual connections are permitted or prohibited for WLAN client devices, and enforce these policies through the appropriate security controls. * Ensure that the organization’s WLAN client devices and APs have configurations at all times that are compliant with the organization’s WLAN policies. * Perform both attack monitoring and vulnerability monitoring to support WLAN security. * Conduct regular periodic technical security assessments for the organization’s WLANs.   **SP 800-44** **Guidelines on Security Public Web Servers**  Organizations should implement appropriate security management practices and controls when maintaining and operating a secure Web server.  **SP 800-127 Guide to Securing WiMAX Wireless Communications**  Organizations should develop a robust WMAN security policy and enforce it.  **SP 800-120 Recommendations for EAP Methods Used in Wireless Network Access Authentication**  This Recommendation formalizes a set of core security requirements for EAP methods when employed by the U.S. Federal Government for wireless access authentication and key establishment. The requirements **should** be considered as generic, in the sense that they are independent of specific wireless technologies. When there are differences between this Recommendation and the referenced IEEE and IETF standards, this Recommendation **shall** have precedence for U.S. Government applications. This Recommendation addresses the validation of a few selected EAP methods, in order to explain the requirements.  See also SP 800-42 Guideline on Network Security Testing and  SP 800-111 Guide to SSL VPNs |
| 2.12 | Encryption and decryption (Addressable) [45 CFR *§* 164.312(a)(2)(iv)]  Implement a mechanism to encrypt and decrypt electronic protected health information.  Federal Register / Vol. 74, No. 79 / Monday, April 27, 2009 Pages 19009  *(II)(B) –* Protected health information (PHI) is rendered unusable, unreadable, or indecipherable to unauthorized individuals only if one or more of the following applies: | **4 – Data Protection and User Access Control**  (d)(1) **Encryption & Cryptographic Controls**  An entity shall utilize encryption to the level appropriate to the data being protected, and where appropriate, to protect individual health information. Entities shall utilize the *NIST Cryptographic Module Validation Program (CMVP)* as the authoritative source of which products, modules, and modes are approved for use by NIST for Federal information Processing. This list, or it’s successor, should be periodically reviewed for updated information as part of each organizations’ internal best practices.  *[45 CFR § 164.312 (a)(2)(iv)], HITECH Breach Notification Law, and the NIST CMVP,* [*http://csr* *c.nist.gov/groups/STM/cmvp/index.html*](http://csrc.nist.gov/groups/STM/cmvp/index.html) | **SP 800-57 Recommendation for Key Management**  1.1 Purpose  Part 3 of the *Recommendation for Key Management, Application-Specific Key Management Guidance,* is intended to address the key management issues associated with currently available cryptographic mechanisms. *General Guidance,* Part 1 of the *Recommendation for Key Management,* contains basic key management guidance for users, developers and system managers regarding the "best practices" associated with the generation and use of the various classes of cryptographic keying material.  See also:  SP 800-67 Rev. 1 DRAFT Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher  SP 800-132 Recommendation for Password-Based Key Derivation  SP 800-131 A & B DRAFT Transitions: Validation of Transitioning Cryptographic Algorithm and Key Lengths  SP 800-130 DRAFT A Framework for Designing Cryptographic Key Management Systems  *SP 800-111* Guide to Storage Encryption Technologies for End User Devices  SP 800-53 Recommended Security Controls for Federal Information Systems and Organizations.  See FIPS 197. |
| 2.13 | **Integrity Controls (Addressable) [45 CFR *§* 164.312(e)(2)(i)]** Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of. | **4 – Data Protection and User Access Control**  **(b)(2) Integrity Controls** - An entity shall implement security measures to safeguard electronically transmitted individual health information from being modified without detection until disposed. This includes implementation of electronic mechanisms to corroborate that individual health information has not been altered or destroyed in an unauthorized manner.  *[45 CFR §§ 164.312 (e)(2)(i) &* *164.312 (c)(2)]* | **NIST SP 800-47 Federal Security Guide for Interconnecting Information Technology Systems**  The Security Guide for Interconnecting Information Technology Systems provides guidance for planning, establishing, maintaining, and terminating interconnections between information technology (IT) systems that are owned and operated by different organizations.  Appendix A Interconnection Security Agreement  The organizations that own and operate the connected information technology (IT) systems should develop an Interconnection Security Agreement (ISA) (or an equivalent document) to document the technical requirements of the interconnection.  A sample agreement is provided in this Appendix.  See also:  SP 800-94 Guide to Intrusion Detection and Prevention Systems (IDPS) |
| 2.14 | **Implementation specification: Mechanism to authenticate electronic protected health information (Addressable) [45 CFR *§* 164.312(c)(2)]** Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner. | Same as immediately above. | **SP 800-47 Security Guide for Interconnecting Information Technology Systems**  The Security Guide for Interconnecting Information Technology Systems provides guidance for planning, establishing, maintaining, and terminating interconnections between information technology (IT) systems that are owned and operated by different organizations.  Appendix A Interconnection Security Agreement  The organizations that own and operate the connected information technology (IT) systems should develop an Interconnection Security Agreement (ISA) (or an equivalent document) to document the technical requirements of the interconnection.  A sample agreement is provided in this Appendix.  See also:  SP 800-94 Guide to Intrusion Detection and Prevention Systems (IDPS)  800-123 Guide to General Server Security  SP 800-53 Recommended Security Controls for Federal Information Systems and Organizations. |