Appendix E—HIPAA Security Rule/FISMA Requirements Crosswalk

This appendix provides a crosswalk of the Administrative, Technical and Physical standards and implementation specifications of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule[123] to the requirements of the Federal Information Security Management Act of 2002 (FISMA), which contains requirements relevant to the security programs of all federal agencies.

Table E-1. HIPAA Security Rule/FISMA Requirements Crosswalk

ADMINISTRATIVE SAFEGUARDS			
164.308(a)(1)(i)	**Security Management Process: Implement policies and procedures to prevent, detect, contain, and correct security violations.**	**Ref §3544(a)(b)(1)** "Periodic assessments of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency."	HIPAA and FISMA require evaluation or implementation of similar safeguards.
164.308(a)(1)(ii)(A)	Risk Analysis (R): Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.	**Ref §3544(a)(b)(1)** "Periodic assessments of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency."	HIPAA and FISMA require evaluation or implementation of similar safeguards
164.308(a)(1)(ii)(B)	Risk Management (R): Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a).	**Ref §3544(b)(2)** "policies and procedures that—(A) are based on the risk assessments required by paragraph (1);(B) cost-effectively reduce information security risks to an acceptable level; (C) ensure that information security is addressed throughout the life cycle of each agency information system; and (D) ensure compliance with—(i) the requirements of this subchapter; (ii)	HIPAA and FISMA require evaluation or implementation of similar safeguards

[123] This crosswalk does not address the administrative and organizational requirements of the HIPAA Security Rule such as those described in Chapter 4. These activities are generally specific to demonstrating compliance with the HIPAA Security Rule rather than standards requiring the implementation of security controls, as is required by FISMA.

[124] In addition to NIST 800-26, specifically mentioned in OMB Memorandum M-03-19, NIST SP 800-53 also includes a set of controls that are required by FISMA and that are relevant to the security controls addressed in the Table E-1 above.

		policies and procedures as may be prescribed by the Director, and information security standards promulgated under section 11331 of title 40; (iii) minimally acceptable system configuration requirements, as determined by the agency; and (iv) any other applicable requirements, including standards and guidelines for national security systems issued in accordance with law and as directed by the President...."	
164.308(a)(1)(ii)(C)	Sanction Policy (R): Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.	**NIST SP 800-26, Appendix A** "Personnel Security: ... 6.1.5 Are mechanisms in place for holding users responsible for their actions?"	Use of either NIST 800-26, *Security Self-Assessment Guide for Information Technology Systems* (November 2001), or an agency-developed guide containing all elements of NIST 800-26, is mandated by OMB Memorandum M-03-19, Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting (August 6, 2003).
164.308(a)(1)(ii)(D)	Information System Activity Review (R): Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	**NIST SP 800-26, Appendix A** "Data Integrity: 11.2.5. Are intrusion detection tools installed on the system? 11.2.6 Are the intrusion detection reports routinely reviewed and suspected incidents handled accordingly? 11.2.7 Is system performance monitoring used to analyze system performance logs in real time to look for availability problems, including active attacks?" "Audit Trails: 17.1 Critical Element: Is activity involving access to a modification of sensitive or critical files logged, monitored, and possible security violations investigated? 17.1.1 Does the audit trail provide a trace of user actions?...17.1.2. Can the audit trail support after-the-fact investigations of how, when, and why normal operations ceased? 17.1.6. Are audit trails reviewed frequently?...17.1.7. Are automated tools used to review audit records in real time or near real time?"	Use of either NIST 800-26, *Security Self-Assessment Guide for Information Technology Systems* (November 2001), or an agency-developed guide containing all elements of NIST 800-26, is mandated by OMB Memorandum M-03-19, Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting (August 6, 2003).

164.308(a)(2)	**Assigned Security Responsibility: Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.**	**Ref §3544(a)(3)** "delegate to the agency Chief Information Officer established under section 3506 (or comparable official in an agency not covered by such section) the authority to ensure compliance with the requirements imposed on the agency under this sub-chapter, including—"(A) designating a senior agency information security officer...."	HIPAA and FISMA require evaluation or implementation of similar safeguards.
164.308(a)(3)(i)	**Workforce Security: Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.**	**NIST SP 800-26, Appendix A** "Personnel Security: 6.1.8 Is there a process for requesting, establishing, issuing, and closing user accounts?"	Use of either NIST 800-26, *Security Self-Assessment Guide for Information Technology Systems* (November 2001), or an agency-developed guide containing all elements of NIST 800-26, is mandated by OMB Memorandum M-03-19, Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting (Aug 6, 2003).
164.308(a)(3)(ii)(A)	Authorization and/or Supervision (A): Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.	**NIST SP 800-26, Appendix A** "Personnel Security: ... 6.1 Critical Element: Are duties separated to ensure least privilege and individual accountability? ... 6.1.2 Are there documented job descriptions that accurately reflect assigned duties and responsibility and that segregate duties?...6.1.5 Are mechanisms in place for holding users responsible for their actions?"	Use of either NIST 800-26, *Security Self-Assessment Guide for Information Technology Systems* (November 2001), or an agency-developed guide containing all elements of NIST 800-26, is mandated by OMB Memorandum M-03-19, Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting (August 6, 2003).
164.308(a)(3)(ii)(B)	Workforce Clearance Procedure (A): Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.	**NIST SP 800-26, Appendix A** "Personnel Security: ... 6.2 Critical Element: Is appropriate background screening for assigned positions completed prior to granting access? 6.2.1 Are individuals who are authorized to bypass significant technical and operational controls screened prior to access and periodically thereafter? 6.2.2 Are confidentiality or security agreements required for employees assigned to work with sensitive information? 6.2.3 When controls cannot adequately protect the information, are individuals screened prior to access?	Use of either NIST 800-26, *Security Self-Assessment Guide for Information Technology Systems* (November 2001), or an agency-developed guide containing all elements of NIST 800-26, is mandated by OMB Memorandum M-03-19, Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting (August 6, 2003).

		6.2.4 Are there conditions for allowing system access prior to completion of screening?"	
164.308(a)(3)(ii)(C)	Termination Procedure (A): Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.	**NIST SP 800-26, Appendix A** "Personnel Security: ... 6.1.7. Are hiring, transfer, and termination procedures established? 6.1.8 Is there a process for requesting, establishing, issuing, and closing user accounts?"	Use of either NIST 800-26, *Security Self-Assessment Guide for Information Technology Systems* (November 2001), or an agency-developed guide containing all elements of NIST 800-26, is mandated by OMB Memorandum M-03-19, Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting (August 6, 2003).
164.308(a)(4)(i)	**Information Access Management: Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.**	**Ref §3544(b)(2)** "policies and procedures that—(A) are based on the risk assessments required by paragraph (1);(B) cost-effectively reduce information security risks to an acceptable level; (C) ensure that information security is addressed throughout the life cycle of each agency information system; and (D) ensure compliance with—(i) the requirements of this subchapter; (ii) policies and procedures as may be prescribed by the Director, and information security standards promulgated under section 11331 of title 40; (iii) minimally acceptable system configuration requirements, as determined by the agency; and (iv) any other applicable requirements, including standards and guidelines for national security systems issued in accordance with law and as directed by the President...."	HIPAA and FISMA require evaluation or implementation of similar safeguards.
164.308(a)(4)(ii)(A)	Isolating Health Care Clearinghouse Functions (R): If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.	**NIST SP 800-26, Appendix A** "Risk Management: 1.1.1 Is the current system configuration documented, including links to other systems?" "Review of Security Controls: 2.1 Critical Element: Have the security controls of the system and interconnected systems been reviewed?" "Authorize Processing (C&A): 4.1.8 Has management authorized interconnections to all systems (including systems owned and operated by another program, agency, organization, or	Use of either NIST 800-26, *Security Self-Assessment Guide for Information Technology Systems* (November 2001), or an agency-developed guide containing all elements of NIST 800-26, is mandated by OMB Memorandum M-03-19, Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting (August 6, 2003).

		contractor)?" "Hardware and System Software Maintenance: 10.1.4 Is the operating system configured to prevent circumvention of the security software and application controls?" "Identification and Authentication: 15.1 Critical Element: Are users individually authenticated via passwords, tokens, or other devices?"	
164.308(a)(4)(ii)(B)	Access Authorization (A): Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.	**NIST SP 800-26, Appendix A** "Identification and Authentication: 15.1 Critical Element: Are users individually authenticated via passwords, tokens, or other devices? 15.1.1 Is a current list maintained and approved of authorized users and their access?"	Use of either NIST 800-26, *Security Self-Assessment Guide for Information Technology Systems* (November 2001), or an agency-developed guide containing all elements of NIST 800-26, is mandated by OMB Memorandum M-03-19, Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting (August 6, 2003).
164.308(a)(4)(ii)(C)	Access Establishment and Modification (A): 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.	**NIST SP 800-26, Appendix A** "Identification and Authentication: 15.1 critical Element: Are users individually authenticated via passwords, tokens, or other devices? 15.1.1 Is a current list maintained and approved of authorized users and their access?" "Logical Access Controls: 16.1 Critical Element: Do the logical access controls restrict users to authorized transactions and functions? 16.1.1. Can the security controls detect unauthorized access attempts?"	Use of either NIST 800-26, *Security Self-Assessment Guide for Information Technology Systems* (November 2001), or an agency-developed guide containing all elements of NIST 800-26, is mandated by OMB Memorandum M-03-19, Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting (August 6, 2003).
164.308(a)(5)(i)	**Security Awareness and Training: Implement a security awareness and training program for all members of its workforce (including management).**	**Ref §3544(b)(4)** "security awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the agency, of—(A) information security risks associated with their activities; and (B) their responsibilities in complying with agency policies and procedures designed to reduce these risks...."	HIPAA and FISMA require evaluation or implementation of similar safeguards.

164.308(a)(5)(ii)(A)	Security Reminders (A):Periodic security updates.	**NIST SP 800-26, Appendix A** "Security Awareness, Training, and Education: 13.1.3 Is there mandatory annual refresher training? 13.1.4 Are methods employed to make employees aware of security, i.e., posters, booklets?"	Use of either NIST 800-26, *Security Self-Assessment Guide for Information Technology Systems* (November 2001), or an agency-developed guide containing all elements of NIST 800-26, is mandated by OMB Memorandum M-03-19, Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting (August 6, 2003).
164.308(a)(5)(ii)(B)	Protection from Malicious Software (A): Procedures for guarding against, detecting, and reporting malicious software.	**NIST SP 800-26, Appendix A** "Data Integrity: 11.1 Critical Element: Is virus detection and elimination software installed and activated? 11.1.1 Are virus signature files routinely updated? 11.1.2 Are virus scans automatic?"	Use of either NIST 800-26, *Security Self-Assessment Guide for Information Technology Systems* (November 2001), or an agency-developed guide containing all elements of NIST 800-26, is mandated by OMB Memorandum M-03-19, Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting (August 6, 2003).
164.308(a)(5)(ii)(C)	Log-in Monitoring (A): Procedures for monitoring log-in attempts and reporting discrepancies.	**NIST SP 800-26, Appendix A** "Logical Access Controls: 16.1 Critical Element: Do the logical access controls restrict users to authorized transactions and functions? 16.1.1 Can the security controls detect unauthorized access attempts? ... 16.1.10 Is access monitored to identify apparent security violations and are such events investigated?"	Use of either NIST 800-26, *Security Self-Assessment Guide for Information Technology Systems* (November 2001), or an agency-developed guide containing all elements of NIST 800-26, is mandated by OMB Memorandum M-03-19, Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting (August 6, 2003).
164.308(a)(5)(ii)(D)	Password Management (A):Procedures for creating, changing, and safeguarding passwords.	**NIST SP 800-26, Appendix A** "Identification and Authentication: 15.1 Critical Element: Are users individually authenticated via passwords, tokens, or other devices?...Are passwords changed at least every ninety days or earlier if needed? 15.1.7 Are passwords unique and difficult to guess (e.g., do passwords require alpha numeric, upper/lower case, and special characters)? 10 Are there procedures in place for handling lost and compromised passwords?	Use of either NIST 800-26, *Security Self-Assessment Guide for Information Technology Systems* (November 2001), or an agency-developed guide containing all elements of NIST 800-26, is mandated by OMB Memorandum M-03-19, Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting (August 6, 2003).

		15.1.11 Are passwords distributed securely and users informed not to reveal their passwords to anyone (social engineering)?"	
164.308(a)(6)(i)	**Security Incident Procedures: Implement policies and procedures to address security incidents.**	**Ref §3544(b)(7)** "procedures for detecting, reporting, and responding to security incidents, consistent with standards and guidelines issued pursuant to section 3546(b), including—(A) mitigating risks associated with such incidents before substantial damage is done; (B) notifying and consulting with the Federal information security incident center referred to in section 3546; and (C) notifying and consulting with, as appropriate—(i) law enforcement agencies and relevant Offices of Inspector General; (ii) an office designated by the President for any incident involving a national security system; and (iii) any other agency or office, in accordance with law or as directed by the President...."	HIPAA and FISMA require evaluation or implementation of similar safeguards.
164.308(a)(6)(ii)	Response and Reporting (R): Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.	**Ref §3544(b)(7)** "procedures for detecting, reporting, and responding to security incidents, consistent with standards and guidelines issued pursuant to section 3546(b), including—"(A) mitigating risks associated with such incidents before substantial damage is done; (B) notifying and consulting with the Federal information security incident center referred to in section 3546; and (C) notifying and consulting with, as appropriate—'(i) law enforcement agencies and relevant Offices of Inspector General;' (ii) an office designated by the President for any incident involving a national security system; and (iii) any other agency or office, in accordance with law or as directed by the President..."	HIPAA and FISMA require evaluation or implementation of similar safeguards.
164.308(a)(7)(i)	**Contingency Plan: Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health**	**Ref §3544(b)(8)** "...plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency."	HIPAA and FISMA require evaluation or implementation of similar safeguards.

	information.		
164.308(a)(7)(ii)(A)	Data Backup Plan (R): Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.	**NIST SP 800-26, Appendix A** "Contingency Planning: ... 9.1.1 Are critical data files and operations identified and the frequency of file backup documented? ... 9.2.5 Is the location of stored backups identified? ...Are backup files created on a prescribed basis and rotated offsite often enough to avoid disruption if current files are damaged?"	Use of either NIST 800-26, *Security Self-Assessment Guide for Information Technology Systems* (November 2001), or an agency-developed guide containing all elements of NIST 800-26, is mandated by OMB Memorandum M-03-19, Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting (August 6, 2003).
164.308(a)(7)(ii)(B)	Disaster Recovery Plan (R): Establish (and implement as needed) procedures to restore any loss of data.	**Ref §3544(b)(8)** "...plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency."	HIPAA and FISMA require evaluation or implementation of similar safeguards.
164.308(a)(7)(ii)(C)	Emergency Mode Operation Plan (R): Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.	**Ref §3544(b)(8)** "...plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency."	HIPAA and FISMA require evaluation or implementation of similar safeguards.
164.308(a)(7)(ii)(D)	Testing and Revision Procedure (A): Implement procedures for periodic testing and revision of contingency plans.	**NIST SP 800-26, Appendix A** "Contingency Planning: 9.3 Critical Element: Are tested contingency/disaster recovery plans in place? ... 9.3.3 Is the plan periodically tested and readjusted as appropriate?"	Use of either NIST 800-26, *Security Self-Assessment Guide for Information Technology Systems* (November 2001), or an agency-developed guide containing all elements of NIST 800-26, is mandated by OMB Memorandum M-03-19, Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting (August 6, 2003).
164.308(a)(7)(ii)(E)	Applications and Data Criticality Analysis (A): Assess the relative criticality of specific applications and data in support of other contingency plan components.	**NIST SP 800-26, Appendix A** "Contingency Planning: 9.1 Critical Element: Have the most critical and sensitive operations and their supporting computer resources been identified? ... 9.1.1 Are critical data files and operations identified and the frequency of file backup documented?"	Use of either NIST 800-26, *Security Self-Assessment Guide for Information Technology Systems* (November 2001), or an agency-developed guide containing all elements of NIST 800-26, is mandated by OMB Memorandum M-03-19, Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting (August 6,

			2003).
164.308(a)(8)	**Evaluation: Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart.**	**Ref §3544(b)(6)** "a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency." **Ref §3545(a)(1)** "Each year each agency shall have performed an independent evaluation of the information security program and practices of that agency to determine the effectiveness of such program and practices."	HIPAA and FISMA require evaluation or implementation of similar safeguards.
164.308(b)(1)	**Business Associate Contracts and Other Arrangements: A covered entity, in accordance with § 164.306, may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with Sec. 164.314(a) that the business associate will appropriately safeguard the information.**	**Ref §3544(a)(1)(A)(ii)** states that the head of each agency shall be responsible for "...information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency"	HIPAA and FISMA require evaluation or implementation of similar safeguards.
164.308(b)(4)	Written Contract or Other Arrangement (R): Document the satisfactory assurances required by paragraph (b)(1) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of **§** 164.314(a).	**NIST 800-26, Appendix A** "Contingency Planning: 9.1 Critical Element: Have the most critical and sensitive operations and their supporting computer resources been identified? ... 9.1.1 Are critical data files and operations identified and the frequency of file backup documented?" "Authorize Processing (C&A): 4.1.8 Has management authorized interconnections to all systems (including systems owned and operated by another program, agency, organization, or contractor)?"	Use of either NIST 800-26, *Security Self-Assessment Guide for Information Technology Systems* (November 2001), or an agency-developed guide containing all elements of NIST 800-26, is mandated by OMB Memorandum M-03-19, Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting (August 6, 2003).

Physical Safeguards			
164.310(a)(1)	**Facility Access Controls: 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.**	**Ref §3544(b)(3)** "subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate" **Ref §3544(b)(8)** "plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency."	HIPAA and FISMA require evaluation or implementation of similar safeguards.
164.310(a)(2)(i)	Contingency Operations (A): Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.	**Ref §3544(b)(3)** "subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate." **Ref §3544(b)(8)** "plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency."	HIPAA and FISMA require evaluation or implementation of similar safeguards.
164.310(a)(2)(ii)	Facility Security Plan (A): Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.	**Ref §3544(b)(3)** "subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate." **Ref §3544(b)(8)** "plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency."	HIPAA and FISMA require evaluation or implementation of similar safeguards.
164.310(a)(2)(iii)	Access Control and Validation Procedures (A): Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.	**Ref §3544(b)(3)** "subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate." **Ref §3544(b)(8)** "plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency."	HIPAA and FISMA require evaluation or implementation of similar safeguards.
164.310(a)(2)(iv)	Maintenance Records (A): Implement policies and procedures to document repairs and modifications to the physical components of a facility, which that are related to security (for example, hardware, walls, doors, and locks).	**Ref §3544(b)(3)** "subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate" AND **Ref §3544(b)(8)** "plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency."	HIPAA and FISMA require evaluation or implementation of similar safeguards.
164.310(b)	**Workstation Use: Implement policies and procedures that specify the proper functions to**	**Ref §3544(a)(1)(A)** "providing information security protections commensurate with the risk and	HIPAA and FISMA require evaluation or implementation of similar safeguards.

	be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.	magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—(i) information collected or maintained by or on behalf of the agency; and (ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency." **Ref §3544(b)(3)** "subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate."	
164.310(c)	**Workstation Security: Implement physical safeguards for all workstations that access electronic protected health information to restrict access to authorized users.**	**Ref §3544(a)(1)(A)** "providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—(i) information collected or maintained by or on behalf of the agency; and (ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency." **Ref §3544(b)(3)** "subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate."	HIPAA and FISMA require evaluation or implementation of similar safeguards.
164.310(d)(1)	**Device and Media Controls: 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.**	**Ref §3544(a)(1)(A)** "providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—(i) information collected or maintained by or on behalf of the agency; and (ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency." **Ref §3544(b)(3)** "subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate."	HIPAA and FISMA requirements require evaluation or implementation of similar safeguards.

164.310(d)(2)(i)	Disposal (R): 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.	**NIST SP 800-26, Appendix A** "Disposal Phase: 3.2.11 Are official electronic records properly disposed/archived?"	Use of either NIST 800-26, *Security Self-Assessment Guide for Information Technology Systems* (November 2001), or an agency-developed guide containing all elements of NIST 800-26, is mandated by OMB Memorandum M-03-19, Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting (August 6, 2003).
164.310(d)(2)(ii)	Media Re-Use (R): Implement procedures for removal of electronic protected health information from electronic media before the media are made available for reuse.	**NIST 800-26, Appendix A** "Disposal Phase: 3.2.12 Is information or media purged, overwritten, degaussed, or destroyed when disposed or used elsewhere?"	Use of either NIST 800-26, *Security Self-Assessment Guide for Information Technology Systems* (November 2001), or an agency-developed guide containing all elements of NIST 800-26, is mandated by OMB Memorandum M-03-19, Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting (August 6, 2003).
164.310(d)(2)(iii)	Accountability (A): Maintain a record of the movements of hardware and electronic media and any person responsible therefore.	**NIST SP 800-26, Appendix A** "Disposal Phase:... 3.2.13 Is a record kept of who implemented the disposal actions and verified that the information or media was sanitized?"	Use of either NIST 800-26, *Security Self-Assessment Guide for Information Technology Systems* (November 2001), or an agency-developed guide containing all elements of NIST 800-26, is mandated by OMB Memorandum M-03-19, Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting (August 6, 2003).
164.310(d)(2)(iv)	Data Backup and Storage (A): Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.	**NIST SP 800-26, Appendix A** "Contingency Planning: ... 9.1.1 Are critical data files and operations identified and the frequency of file backup documented? ... 9.2.5 Is the location of stored backups identified? ... Are backup files created on a prescribed basis and rotated offsite often enough to avoid disruption if current files are damaged?"	Use of either NIST 800-26, *Security Self-Assessment Guide for Information Technology Systems* (November 2001), or an agency-developed guide containing all elements of NIST 800-26, is mandated by OMB Memorandum M-03-19, Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting (August 6, 2003).

Technical Safeguards			
164.312(a)(1)	**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 § 164.308(a)(4).**	**Ref §3544(a)(1)(A)** "providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—(i) information collected or maintained by or on behalf of the agency; and (ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency." **Ref §3544(b)(3)** "subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate."	HIPAA and FISMA requirements require evaluation or implementation of similar safeguards.
164.312(a)(2)(i)	Unique User Identification (R): Assign a unique name and/or number for identifying and tracking user identity.	**NIST SP 800-26, Appendix A** "Identification and Authentication: 15.1 Critical Element: Are users individually authenticated via passwords, tokens, or other devices?...Are passwords changed at least every ninety days or earlier if needed? 15.1.7 Are passwords unique and difficult to guess (e.g., do passwords require alpha numeric, upper/lower case, and special characters)?" "Logical Access Controls: 16.1.10 Is access monitored to identify apparent security violations and are such events investigated?"	Use of either NIST 800-26, *Security Self-Assessment Guide for Information Technology Systems* (November 2001), or an agency-developed guide containing all elements of NIST 800-26, is mandated by OMB Memorandum M-03-19, Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting (August 6, 2003).
164.312(a)(2)(ii)	Emergency Access Procedure (R): Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.	**NIST SP 800-26, Appendix A** "Identification and Authentication: 15.1.4 Is emergency and temporary access authorized?"	Use of either NIST 800-26, *Security Self-Assessment Guide for Information Technology Systems* (November 2001), or an agency-developed guide containing all elements of NIST 800-26, is mandated by OMB Memorandum M-03-19, Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting (August 6, 2003).

164.312(a)(2)(iii)	Automatic Logoff (A): Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	**NIST SP 800-26, Appendix A** "Logical Access Controls: 16.1.4 Do workstations disconnect or screensavers lock system after a specific period of inactivity?"	Use of either NIST 800-26, *Security Self-Assessment Guide for Information Technology Systems* (November 2001), or an agency-developed guide containing all elements of NIST 800-26, is mandated by OMB Memorandum M-03-19, Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting (August 6, 2003).
164.312(a)(2)(iv)	Encryption and Decryption (A): Implement a mechanism to encrypt and decrypt electronic protected health information.	**Ref §3544(a)(1)(A)** "providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—(i) information collected or maintained by or on behalf of the agency; and (ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency." **Ref §3544(b)(3)** "subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate." **NIST SP 800-26, Appendix A** "Logical Access Controls: 16.1.7 If encryption is used, does it meet Federal standards? 16.1.8 If encryption is used, are there procedures for key generation, distribution, storage, use, destruction, and archiving? ...16.2.14 Are sensitive data transmissions encrypted?"	HIPAA and FISMA requirements require evaluation or implementation of similar safeguards; specific standards are required if encryption is deemed necessary and implemented
164.312(b)	**Audit Controls: Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.**	**Ref §3544(a)(1)(A)** "providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—(i) information collected or maintained by or on behalf of the agency; and (ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an	HIPAA and FISMA requirements require evaluation or implementation of similar safeguards.

		agency." **Ref §3544(b)(3)** "subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate."	
164.312(c)(1)	**Integrity: Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.**	**Ref §3544(a)(1)(A)** "providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—(i) information collected or maintained by or on behalf of the agency; and (ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency." **Ref §3544(b)(3)** "subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate."	HIPAA and FISMA requirements require evaluation or implementation of similar safeguards.
164.312(c)(2)	Mechanism to Authenticate Electronic Protected Health Information (A): Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.	**NIST SP 800-26, Appendix A** "Data Integrity: 11.2 Critical Element: Are data integrity and validation controls used to provide assurance that the information has not been altered and the system functions as intended? 11.2.1 Are reconciliation routines used by applications, i.e., checksums, hash totals, record counts? 11.2.4 Are integrity verification programs used by applications to look for evidence of data tampering, errors, and omissions? ... 11.2.9 Is message authentication used?"	Use of either NIST 800-26, *Security Self-Assessment Guide for Information Technology Systems* (November 2001), or an agency-developed guide containing all elements of NIST 800-26, is mandated by OMB Memorandum M-03-19, Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting (August 6, 2003).
164.312(d)	**Person or Entity Authentication: Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.**	**Ref §3544(a)(1)(A)** "providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—(i) information collected or maintained by or on behalf of the agency; and (ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency." **Ref §3544(b)(3)** "subordinate plans for providing adequate information security for networks, facilities, and systems or	HIPAA and FISMA requirements require evaluation or implementation of similar safeguards.

		groups of information systems, as appropriate."	
164.312(e)(1)	**Transmission Security: Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.**	**Ref §3544(a)(1)(A)** "providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—(i) information collected or maintained by or on behalf of the agency; and (ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency." **Ref §3544(b)(3)** "subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate."	HIPAA and FISMA requirements require evaluation or implementation of similar safeguards.
164.312(e)(2)(i)	Integrity Controls (A): Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.	**NIST SP 800-26, Appendix A** "Data Integrity: 11.2 Critical Element: Are data integrity and validation controls used to provide assurance that the information has not been altered and the system functions as intended? 11.2.1 Are reconciliation routines used by applications, i.e., checksums, hash totals, record counts? 11.2.4 Are integrity verification programs used by applications to look for evidence of data tampering, errors, and omissions? ... 11.2.9 Is message authentication used?"	Use of either NIST 800-26, *Security Self-Assessment Guide for Information Technology Systems* (November 2001), or an agency-developed guide containing all elements of NIST 800-26, is mandated by OMB Memorandum M-03-19, Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting (August 6, 2003).
164.312(e)(2)(ii)	Encryption (A): Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	**Ref §3544(a)(1)(A)** "providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—(i) information collected or maintained by or on behalf of the agency; and (ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency." **Ref §3544(b)(3)** "subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate." **NIST SP 800-26, Appendix A**	HIPAA and FISMA requirements require evaluation or implementation of similar safeguards; specific standards are required if encryption is deemed necessary and implemented

		"Logical Access Controls: 16.1.7 If encryption is used, does it meet federal standards? 16.1.8 If encryption is used, are there procedures for key generation, distribution, storage, use, destruction, and archiving? ...16.2.14 Are sensitive data transmissions encrypted?"	