Summary of Security Standards

Common Name	**FISMA**	**SOX**	**HIPPA**	**CMS CSR**
Long Name	Federal Information Security Management Act (FISMA)	Sarbanes Oxley Act	Health Insurance Portability and Accountability Act of 1996	CMS Core Security Requirements
Authority	Title III of the E-Government Act of 2002	Section 302 & 404 of the Sarbanes Oxley Act of 2002 (Public Law 107-204)	Health Insurance Portability and Accountability Act of 1996	"Medicare Prescription Drug, Improvement, and Modernization Act of 2003 - SEC. 912: Requirements for Information Security for Medicare Administrative Contractors" (Section 912 of the MMA)
General Description	Provides for assigning the risk of operating a system processing federal data to a Federal Executive and includes direction for establishing procedures and standards and guidance for: -The categorization of information and information systems by mission impact -The minimum security requirements for information and information systems -The selection of appropriate security controls for information systems	The act mandates the establishment of internal controls on financial systems to assure the accuracy and integrity of the processing of those systems. A statement attesting to the adequacy of the controls is required in the annual report. The act establishes the Public Company Accounting Oversight Board (PCAOB) to administer and enforce SOX. The act includes provisions for	The Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Title II) required the Department of Health and Human Services (HHS) to establish national standards for electronic health care transactions and national identifiers for providers, health plans, and employers. It also addressed the security and privacy of health data. Privacy rules are defined by	Defines the controls which must be applied to CMS Business Partner systems and defines the procedures and standards for assessing and certifying the implementation. It appears to be comparable in scope to FISMA and very similar. The "Centers for Medicare & Medicaid Services (CMS) Business Partners Systems Security Manual" is the defining document.

	-The assessment of security controls in information systems and determining security control effectiveness -The process for certifying and accrediting information systems The FISMA assessment process addresses policy, process & procedure and technical control implementation.	the establishment of standards and guidelines for identifying the necessary controls and assessing those controls. The SOX primary concern is the integrity of the data used to produce the annual report.	the Privacy Rule which applies to all forms of Personal Health Information (PHI). The security rules are defined by The Security Rule and apply only to Electronic PHI (EPHI). The security rule specifies a series of administrative, technical, and physical security procedures for covered entities to use to assure the confidentiality of electronic protected health information. The security rule requires an initial and periodic risk based assessment of the system However, there appear to be no rigid standards for assessing the implementation of the standards.	
Covered Entities	"… the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source."	Registered Public Corporations The act actually directs public accounting firms to take certain actions IAW with specific standards in the audit of public companies.	1. A health care provider that conducts certain transactions in electronic form (called a "covered health care provider"). 2. A health care clearinghouse. 3. A health plan.	CMS business partners (contractor), a corporation or organization that contracts with CMS to process or support the processing of Medicare fee-for-service claims.
Related	FIPS 199 (NIST SP 800-60)	Auditing Standard No. 5, An	Security Standards for	

Standards and Guidance	FIPS 200 (NIST SP 800-53) NIST SP 800-53A (Assessment Procedures) NIST SP 800-37 (C&A Process) NIST SP 800-30 (Risk Assessment Procedure) NIST SP 800-34 (Contingency Planning) Appendix III to OMB Circular No. A-130 - Security of Federal Automated Information Resources	Audit of Internal Control Over Financial Reporting That Is Integrated with An Audit of Financial Statements	the Protection of Electronic Protected Health Information", found at 45 CFR Part 160 and Part 164, Subparts A and C. NIST SP 800-66 (HIPPA Implementation Guidance)	
Relationship to Other Standards	The FISMA process encompasses HIPPA and the provisions of the Privacy Act as applicable to a given system.	Independent of FISMA but similar in scope.	Examination of the Security Rule will likely find a resemblance to the FISMA controls.	Includes provisions for FISMA, HIPPA and all privacy regulations.
Comments	FISMA also specifies that a written contingency plan be in place for all systems and test tested annually.	Violations are treated as a violation of the Securities and Exchange Act of 1934, and subject to the same penalties of that Act. Public corporations that contract with the Federal Government can be subject to both FISMA and SOX.	Mandatory provisions can be bypassed if compensating controls exist or if the cost of implementation exceeds the gain in risk reduction. Special provisions also apply for "small" entities.	A well defined process for meeting the contractor C&A provisions of FISMA.
Links for additional information:	NIST - FISMA Appendix III to OMB Circular No. A-130 - Security of Federal	The Sarbanes-Oxley Act 2002 Sarbanes-Oxley Implementation Central	HIPAA.ORG HHS - Office for Civil Rights - HIPAA	Centers for Medicare & Medicaid Services (CMS) Business Partners Systems Security Manual http://www.cms.hhs.gov/Infor

		Internal Control Reporting Provisions	CoveredEntitycharts.pdf (application/pdf Object)	mationSecurity/13_Policies.asp

Other Standards and Regulations to be reviewed:

1. State Laws
2. ISO 17799 Code of Security Practices
3. Privacy Act