

DRAFT Comparison of HIPAA to CMS Core Security Requirements (CMS CSR)

Category	CSR #	Control Technique	45 C.F.R. ____	Comments
	CSR 1.1.1	Security training includes the following topics and the related procedures: (1) awareness training; (2) periodic security reminders; (3) user education concerning malicious software; (4) user education in importance of monitoring log in success/failure and how to report discrepancies; and (5) user education in password management (rules to be followed in creating and changing passwords, and the need to keep them confidential).	164.308(a)(5)(i) 164.308(a)(5)(ii)(A) 164.308(a)(5)(ii)(B) 164.308(a)(5)(ii)(C) 164.308(a)(5)(ii)(D)	
	CSR 1.1.3	All personnel (employees and contractors) are provided security awareness training prior to being allowed access to sensitive information or Medicare data, and then are provided annual security refresher training. The training is customized based on job responsibilities.	164.308(a)(5)(i)	Training before access not specifically required under HIPAA
	CSR 1.1.6	A record of the security awareness training subject(s) covered is maintained.	164.316(b)(1)(ii)	
	CSR 1.2.1	Designated management personnel monitor the testing of corrective security actions after implementation and on a continuing basis.	164.316(b)(2)(iii) 164.308(a)(1)(ii)(D) 164.308(a)(8)	
	CSR 1.3.2	The CMS Business Partner's system is recorded on a separate list that includes: (1) to whom the disclosure was made; (2) what was disclosed; (3) why it was disclosed; and (4) when it was disclosed.	164.312(c)(1) 164.312(c)(2) 164.312(e)(2)(I)	Not specifically required under HIPAA Security
	CSR 1.3.3	Appropriate controls are established for all sensitive data entering or leaving the facility. A system is employed that precludes erroneous or unauthorized transfer of data, regardless of media or format. Include controls that maintain a record for the logging of shipping and receipts and a periodic reconciliation of these records.	164.310(d)(2)(iii) 164.312(e)(1)	
	CSR 1.3.4	A data destruction procedure has been developed for inactive or aged records and files to ensure that sensitive data does not become available to unauthorized personnel.	154.310(d)(2)(I)	

DRAFT Comparison of HIPAA to CMS Core Security Requirements (CMS CSR)

Category	CSR #	Control Technique	45 C.F.R. ____	Comments
	CSR 1.3.5	All retired, discarded, or unneeded sensitive data is disposed in a manner that prevents unauthorized persons from using it. All sensitive data is erased from storage media before releasing as work tapes or disks. Ensure the destruction of any sensitive information hard copy documents when no longer needed.	164.310(d)(2)(i) 164.310(d)(2)(ii)	
	CSR 1.3.7	Sensitive information is never disclosed during disposal unless authorized by statute. Destruction of sensitive information is witnessed by a CMS Business Partner employee. However, a Business Partner may elect to have the destruction certified by a shredding contractor in the absence of Business Partner participation.	164.310(d)(2)(ii) 164.310(d)(2)(iii)	CSR is more specific than HIPAA
	CSR 1.3.8	Before releasing files containing sensitive information to an individual or contractor not authorized to access sensitive information, care is taken to remove all such sensitive information. Procedures are in place to clear sensitive information and software from computers, memory areas, disks, and other equipment or media before they are disposed of or transferred to another use. The responsibility for clearing information is clearly assigned, and standard forms or a log is used to document that all discarded or transferred items are	164.310(d)(2)(i) 164.310(d)(2)(ii) 164.312(c)(1) 164.312(c)(2) 164.312(e)(2)(i) 164.310(d)(2)(iii)	
	CSR 1.3.12	Inventory records of all storage media containing sensitive data must be maintained for purposes of control and accountability. Such storage media, any hard copy printout of such media, or any file resulting from the processing of such media will be recorded in a log that identifies: (1) date received, (2) reel/cartridge control number contents, (3) number of records if available, (4) movement, and (5) if disposed of, the date and method of destruction. Such a log must permit all storage media containing sensitive data (including those	164.310(d)(2)(iii)	
	CSR 1.3.15	Whenever possible computer operations are in a secure area with restricted access. Sensitive information is kept locked when not in use. Tape reels, disks, or other media are labeled as CMS Sensitive Information. Media holding, processing or storing sensitive data is kept in a secure area.	164.310(a)(1) 164.310©	
	CSR 1.4.1	Personnel Security includes all of the following features: (1) assuring supervision of maintenance personnel by an authorized, knowledgeable person; (2) maintaining a record of access authorizations; (3) assuring that operating personnel and maintenance personnel have proper access authorization; (4) establishing personnel clearance procedures; (5) establishing and maintaining personnel security policies and procedures; (6) assuring that system users, including maintenance personnel, receive security awareness training; and (7)	164.308(a)(3)(i) 164.308(a)(3)(ii)(A) 164.308(a)(3)(ii)(B) 164.308(a)(4)(ii)(B) 164.308(a)(4)(ii)(C) 164.308(a)(5)(I)	
	CSR 1.4.2	To provide reasonable assurance that sensitive information is adequately safeguarded, an annual self-assessment is conducted which addresses the safeguard requirements imposed by CMS. A copy of the self-assessment is submitted to CMS.	164.308(a)(8)	HIPAA is not as specific

DRAFT Comparison of HIPAA to CMS Core Security Requirements (CMS CSR)

Category	CSR #	Control Technique	45 C.F.R. ____	Comments
de Security Program Planning and Management	CSR 1.4.3	Reporting Improper Inspections or Disclosures of Sensitive Information - Upon discovery by any employee, the individual making the observation or receiving the information contacts his or her supervisor, who contacts CMS for submission to the appropriate authority.	164.308(a)(6)(ii)	
	CSR 1.4.4	Security policies are distributed to all affected personnel. They include: (1) system and application rules; (2) rules that clearly delineate responsibility; (3) rules that describe expected behavior of all with access to the system; and (4) procedures to prevent, detect, contain, and correct security violations.	164.308(a)(1)(i)	
	CSR 1.4.5	Procedures for employees to follow when they discover a privacy breach or a violation of IS systems security are established. The procedures: (1) stipulate what information employees must provide; (2) whom they must notify; and (3) what degree of urgency to place on reporting the incident. The procedures ensure that reports of possible security violations are accurate and timely.	164.308(a)(6)(i) 164.308(a)(6)(ii)	
	CSR 1.5.2	The security organization designates a System Security Officer (SSO), at an overall level and at appropriate subordinate levels, qualified to manage Medicare system security program and to assure that necessary safeguards are in place and working.	164.308(a)(2)	
	CSR 1.5.5	The SSO assures compliance with CMS's systems security requirements by performing the following: (1) coordinating system security activities for all Medicare components; (2) reviewing compliance of all Medicare components with CMS systems security requirements and reporting vulnerabilities to management; (3) investigating systems security breaches and reporting significant problems to management for review by CMS Regional Officer and/or Consortium; (4) ensuring that internal controls are incorporated into new		
	CSR 1.5.7	Documentation designates specific employees responsible for securing removable storage devices and media containing sensitive information.	164.310(d)(1)	HIPAA is not as specific
	CSR 1.6.1	Procedures exist to identify and report incidents: (1) security incident procedures; (2) report procedures; (3) response procedures; and (4) procedures to regularly review records of information system activity, such as security incident tracking reports.	164.308(a)(1)(ii)(D) 164.308(a)(6)(i)	

DRAFT Comparison of HIPAA to CMS Core Security Requirements (CMS CSR)

Category	CSR #	Control Technique	45 C.F.R. ____	Comments
Entitywide	CSR 1.8.1	Security management process implementation features are available, as follows: (1) risk analysis; (2) risk management; (3) sanction policy and procedures; and (4) security policy.	164.308(a)(1)(ii)(A) 164.308(a)(1)(ii)(B) 164.308(a)(1)(ii)(C)	
	CSR 1.8.2	Final risk determinations and related management approvals are documented and maintained on file. (Such determinations may be incorporated in the system security plan.)	164.308(a)(1)(ii)(A)	HIPAA is not as specific
	CSR 1.8.3	The risk assessment considers data sensitivity and integrity and the range of risks to the entity's systems and data.	164.308(a)(1)(ii)(A)	
	CSR 1.8.4	A risk assessment is conducted whenever significant modifications are made to a system, facility, and network. The risk assessment includes: (1) assets (Medicare funds and data and the hardware, software and facilities involved in processing Medicare claims); (2) risks (Disaster, disruption, unauthorized disclosure, error, theft and fraud); and (3) safeguards (Policy, procedure, separating duties, training, posters/notices/ announcements, testing/validating/editing, audit routines, audit trails/logs, alarms and fire	164.308(a)(1)(ii)(A) 164.308(a)(8)	
	CSR 1.8.5	Facilities housing sensitive and critical resources have been identified. All significant threats to the physical well-being of sensitive and critical resources have been identified and related risks determined.	164.308(a)(1)(ii)(A)	
	CSR 1.9.1	The following are accomplished and documented: (1) security configuration documentation; (2) hardware/software installation and maintenance review and testing for security features; (3) inventory records; (4) security testing; and (5) checking for malicious software.	164.310(d) 164.308(a)(8)	

DRAFT Comparison of HIPAA to CMS Core Security Requirements (CMS CSR)

Category	CSR #	Control Technique	45 C.F.R. ____	Comments
	CSR 1.9.2	Administrative procedures to guard data integrity, confidentiality, and availability include formal mechanisms for processing records.	164.316(a)	
	CSR 1.9.3	A security program plan has been documented that: (1) covers all major facilities and operations; (2) has been approved by key affected parties and covers the topics prescribed by OMB Circular A-130 such as: (a) Rules of the system/Application rules; (b) Training/Specialized training; (c) Personnel controls/Personnel security; (d) Incident response capability; (e) Continuity of support/Contingency planning; (f) Technical security/Technical controls; (g) System interconnection/Information sharing; (h) Public access controls.	164.316	Some is not applicable outside of federal government, and no specific approval provision in HIPAA
	CSR 1.9.5	The CMS Business Partner System Security Profile shall be maintained and consists of the following: (1) description of Medicare operations, records and the resources necessary to process Medicare claims; (2) risk assessment; (3) security plan; (4) certification; (5) self-assessment; (6) contingency plans; (7) security reviews, including those undertaken by OIG, CMS, consultants, subcontractors and internal security audit staff; (8) implementation schedules for safeguards and updates; (9) systems security policies and procedures; (10)		Not applicable outside of CMS
	CSR 1.9.6	Retention procedures are established for all CMS sensitive information.		Not in HIPAA
	CSR 1.9.7	Documentation is available to assure that the level of sensitivity and criticality designations of each system has been assigned and has been determined to be commensurate with the sensitivity of the information and the risk and magnitude of loss or harm that could result from improper operation of the information system.	164.308(a)(7)(ii)(E)	
	CSR 1.9.8	Vulnerability identification is performed on new, existing, and recently modified sensitive systems and facilities. A summary list of vulnerabilities is prepared for each sensitive system and facility being analyzed.	164.308 (A)(1)(II)(a)	
	CSR 1.9.9	The system security plan is reviewed periodically and adjusted to reflect current conditions and risks.	164.308(A)(8)	

DRAFT Comparison of HIPAA to CMS Core Security Requirements (CMS CSR)

Category	CSR #	Control Technique	45 C.F.R. ____	Comments
	CSR 1.10.4	Termination and transfer procedures include: (1) exit interview procedures; (2) return of property, keys, identification cards, passes; (3) notification to security management of terminations and prompt revocation of IDs and passwords; (4) immediately escorting involuntarily terminated employees out of the entity's facilities; and (5) identifying the period during which nondisclosure requirements remain in effect.	164.308(a)(3)(ii)(C)	
	CSR 1.10.6	Confidentiality or security agreements are required for CMS Business Partner Medicare employees and their contractors assigned to work with sensitive information.	164.308(b) 164.314(A)	
	CSR 1.11.2	Written contracts or other arrangements require the inclusion of the CMS Core Security Requirements to protect the integrity, confidentiality, and availability of the electronically exchanged data. The CMS Business Partner will maintain a list of all contracts or other arrangements with other CMS Business Partners or business associates (include organization name and location, contract or agreement number, and purpose). The list of contracts will be provided to CMS in an MS Word document with the annual CAST submission.		Not applicable outside of CMS
	CSR 1.11.3	The CMS Business Partner has obtained satisfactory assurances that all external business associates will provide appropriate safeguards for CMS sensitive information.	164.308(b)(1) 164.314(a)	
	CSR 1.13.1	Policies and procedures are implemented that specify the proper workstation functions to 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 CMS sensitive information.	164.310(b) 164.310©	
	CSR 1.13.4	If CMS Business Partner employees are authorized to work at home on sensitive data, they are required to observe the same security practices that they observe at the office.	164.310(b) 164.310(c)	
	CSR 1.13.5	Policies are established for controlling the use of laptops, notebooks and other mobile computing devices. When authorized for official business to be conducted from the home or other location, the user takes responsibility for safe transit, secure storage, and for assuring no one else uses the device, accessories and media storage, while in his/her custody.	164.310(b) 164.310(c)	

DRAFT Comparison of HIPAA to CMS Core Security Requirements (CMS CSR)

Category	CSR #	Control Technique	45 C.F.R. ____	Comments
	CSR 2.1.1	User account activity audits are conducted using automated audit controls.	164.312(b)	
	CSR 2.1.2	Computers systems processing sensitive information are secured from unauthorized access. All security features are available and activated. Audit facilities are utilized to assure that everyone who accesses a computer system containing sensitive information is accountable.	164.312(a)(1) 164.312(b)	
	CSR 2.1.3	All activity involving access to and modifications of sensitive or critical files is logged.	164.312(b)	
	CSR 2.1.6	Audit trails/logs are reviewed periodically (i.e., minimum of weekly) and retained for a minimum of 60 days.	164.308(a)(1)(ii)(D)	HIPAA does not set minimum review intervals
	2.2.2	Sensitive information (including tapes or cartridges) are placed in secure storage in a secure location, safe from unauthorized access. All containers, rooms, buildings, and facilities containing sensitive information are locked when not in use. Locking systems are planned for and used in conjunction with other security measures.	164.310(a)(1)	No specific locking mechanism requirement in HIPAA
	CSR 2.2.6	Visitors to sensitive areas, such as the main computer room, tape/media library, and restricted areas, are formally signed in and escorted. Restricted area registers are maintained and include: (1) the name; (2) date; (3) time of entry; (4) time of departures; (5) purpose of visit; and (6) who visited. Restricted area register is closed out at the end of each month and reviewed by the area supervisor. For a restricted area, the identity of visitors is verified and a new <u>Authorized Access List (AAL)</u> is issued monthly.	164.308(a)(1)(ii)(D) 164.310(a)(1) 164.310(a)(2)(iii)	No specific register requirement in HIPAA
	CSR 2.2.7	Emergency exit and re-entry procedures ensure that only authorized personnel are allowed to reenter after fire drills, or other evacuation procedures.	164.310(a)(2)(i)	

DRAFT Comparison of HIPAA to CMS Core Security Requirements (CMS CSR)

Category	CSR #	Control Technique	45 C.F.R. ____	Comments
	CSR 2.2.14	Sensitive information is locked in cabinets or sealed in packing cartons while in transit. Sensitive information material remains in the custody of a CMS or CMS Business Partner employee. Accountability is maintained during the move.	164.310(d)(2)(iii)	HIPAA not as specific
	CSR 2.2.15	Key combinations are changed when an employee who knows the combination retires, terminates employment, or transfers to another position. An envelope containing the combination is secured in a container with the same or higher classification as the material the lock secures.	164.308(a)(3)(ii)(C)	HIPAA termination procedures not as specific
	CSR 2.2.17	Physical safeguards to restrict access to authorized users are implemented for all workstations that access CMS sensitive information.	164.310(c)	
	CSR 2.2.21	Access is limited to those individuals who routinely need access through the use of guards, identification badges, or entry devices such as key cards.	164.310(a)(2)(iii) 164.308(a)(4)	
	CSR 2.2.22	Management regularly reviews the list of persons with physical access to sensitive facilities.	164.308(a)(4)(ii)(c) 164.310(a)(2)(iii)	
	CSR 2.2.26	Unauthorized personnel are denied access to areas containing sensitive information during working hours. Methods include use of restricted areas, security rooms, and locked doors.	164.310(a)(2)(iii)	
	CSR 2.2.27	Procedures exist for verifying access authorizations before granting physical access (formal, documented policies and instructions for validating the access privileges of an entity before granting those privileges).	164.310(a)(1) 164.310(a)(2)(iii)	

DRAFT Comparison of HIPAA to CMS Core Security Requirements (CMS CSR)

Category	CSR #	Control Technique	45 C.F.R. ____	Comments
Access Control	CSR 2.2.28	Responsibility is assigned and security procedures are documented for bringing hardware and software into and out of the facility, as well as movement of these items within the facility, and for maintaining a record of those items.	164.310(d)(1) 164.310(d)(2)(iii)	
	CSR 2.2.29	Procedures are implemented to control access to software programs undergoing testing or revision.	164.310(a)(2)(iii)	
	CSR 2.2.30	Policies and procedures are implemented to document repairs and modifications to the physical components of a facility which are related to security (e.g., hardware, walls, doors, and locks).	164.310(a)(2)(iv)	
	CSR 2.4.1	Procedures are established (and implemented as needed) 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.	164.312(a)(2)(i)	
	CSR 2.5.3	Only employees with a valid need-to-know are permitted access and safeguards are sufficient to limit unauthorized access and ensure confidentiality.	164.308(a)(3)(i) 164.308(a)(3)(ii)(A) 164.308(a)(4)(ii)(B) 164.308(a)(4)(ii)(C) 164.312(d) 164.310(a)(1) 164.310(a)(2)(iii)	
	CSR 2.5.8	Inspection reports, including self-assessment reports, corrective actions, and supporting documentation, are to be retained for a minimum of seven (7) years.	164.316(b)(2)(i) 164.316(b)(1)(ii)	HIPAA requires 6 years instead of 7
	CSR 2.6.1	Security violations and activities, including failed log on attempts, other failed access attempts and sensitive activity are identified, reported, and reacted to by intrusion detection software. The identified unauthorized, unusual, and sensitive access activities are reported to management and investigated.	164.308(a)(6)	

DRAFT Comparison of HIPAA to CMS Core Security Requirements (CMS CSR)

Category	CSR #	Control Technique	45 C.F.R. ____	Comments
	CSR 2.6.3	Procedures instruct supervisors: (1) to monitor the activities of visitors to the work area (including CMS Business Partner employees from other work areas); and (2) to ensure that functions of the unit are performed only by employees assigned to the unit. Supervisors shall have procedures for handling questionable activities.	164.310(a)(2)(iii) 164.308(a)(3)(ii)(A)	
	CSR 2.7.2	Access to sensitive information is on a strictly need-to-know basis. Contractors evaluate the need for the sensitive information before the data is requested or disseminated.	164.308(a)(4)(i)	
	CSR 2.8.1	Security is notified immediately when system users are terminated or transferred.	164.308(a)(3)(ii)(C)	Termination procedures are required in HIPAA, but the regulations are not this specific.
	CSR 2.8.8	Documented policies and procedures exist for granting different levels of access to health care information that includes rules for the following: (1) granting of user access; (2) determination of initial rights of access to a terminal, transaction, program, or process; (3) determination of the types of, and reasons for, modification to established rights of access, to a terminal, transaction, program, process.	164.308(a)(4)(ii)(B) 164.308(a)(4)(ii)(C) 164.312(a)(1)	
	CSR 2.9.4	The use of passwords and access control measures are in place to identify who accessed protected information and limit that access to persons with a need-to-know.	164.312(a)(1)	
	CSR 2.9.6	Entity authentication (the corroboration that an entity is the one claimed) exists and includes automatic logoff after a predetermined amount of time (normally 15 minutes) and unique user identifier. It also includes at least one of the following implementation features: (a) biometric identification, (b) password, (c) personal identification number (PIN), or (d) telephone callback procedure.	164.312(a)(2)(i) 164.312(a)(2)(iii) 164.312(d)	
	CSR 2.9.10	Passwords are: (1) unique for specific individuals, not groups; (2) controlled by the assigned user and not subject to disclosure; (3) changed periodically--every 30 to 90 days, when an individual changes positions, or when security is breached; (4) not displayed when entered; (5) at least six alphanumeric characters in length and prohibited from reuse for at least 6 generations.	164.312(a)(2)(I)	HIPAA is not this specific.

DRAFT Comparison of HIPAA to CMS Core Security Requirements (CMS CSR)

Category	CSR #	Control Technique	45 C.F.R. ____	Comments
	CSR 2.9.11	Inactivity at any given workstation for a specific period of time shall cause the system to automatically shut down that workstation. However, in a controlled (supervised) environment, involving the use of sign-on and password routines, there is no "time-out" disconnect requirement. Screensavers with passwords are utilized where supported by existing operating systems.	164.312(a)(2)(iii)	
	CSR 2.9.12	Authorization control (the mechanism for obtaining consent for the use and disclosure of health information) exists and includes at least one of the following implementation features: role-based access or user-based access.	164.308(a)(4)(ii) 164.308(a)(4)(ii)(B)	HIPAA does not specifically require role or user-based access
	CSR 2.9.13	If a CMS business partner is part of a larger organization, the business partner must implement policies and procedures that protect CMS sensitive information from unauthorized access by the larger organization.	164.308(a)(4)(ii)(A)	HIPAA is specific to healthcare clearinghouses, see also 164.105(a)
	CSR 2.10.5	Inactive users accounts are monitored and removed when not needed.	164.308(a)(4)(ii)(C)	
	CSR 2.11.2	Access and changes to DBMS software are controlled.	N/A	
	CSR 2.12.1	Access to sensitive information is limited to those who are authorized by law or regulation. Physical and systemic barriers are reviewed/reported. Assessments are conducted of facility security features.	164.310(a)(1)	
	CSR 2.13	SSOs investigate security violations and report results to appropriate supervisory and management personnel. Appropriate disciplinary actions are taken.	164.308(6) 164.308(a)(1)(ii)(C)	

DRAFT Comparison of HIPAA to CMS Core Security Requirements (CMS CSR)

Category	CSR #	Control Technique	45 C.F.R. ____	Comments
System Software	CSR 2.13.3	Access control policies and techniques are modified when violations and related risk assessments indicate that such changes are appropriate.	164.306(e)	
	CSR 3.1.1	Policy defines investigation of inappropriate or unusual activity and guidelines for appropriate actions to be taken.	164.308(a)(6)(i)	
	CSR 3.1.2	Management reviews are performed to determine that control techniques for monitoring use of sensitive system software are functioning as intended and that the control techniques in place are maintaining risks within acceptable levels (e.g., periodic risk assessments).	164.308(a)(8)	
	CSR 3.1.5	Systems support alarm features to provide immediate notification of predefined events.	N/A	
	CSR 3.6.4	Access to system software is restricted to personnel with corresponding job responsibilities by access control software. Update access is generally limited to primary and backup systems programmers.	164.310(a)(2)(iii)	
	4.2.1	All operator activities on the computer system are recorded on an automated history log.	164.312(b)	But only for ePHI
	4.2.4	Supervisors routinely review the history log and investigate any abnormalities.	164.308(a)(1)(ii)(d)	

DRAFT Comparison of HIPAA to CMS Core Security Requirements (CMS CSR)

Category	CSR #	Control Technique	45 C.F.R. ____	Comments
	4.5.1	Physical and logical access controls help restrict employees to authorized actions, based upon organizational and individual job responsibilities.	164.310(a)(1) 164.312(a)(1)	
Security	CSR 5.2.4	Contingency Plan consists of all components listed in the CMS Business Partner's Systems Security Manual.	N/A	
	CSR 5.2.7	The Contingency Plan emergency response procedures provide for emergency personnel (such as doctors or electricians) to obtain immediate entry to all restricted areas.	164.308(a)(7)(ii)(c) 164.310(a)(2)(i)	
	CSR 5.2.9	Contingency Plans, software procedures, and installed security and backup provisions protect against improper modification of data in the event of a system failure.	164.308(a)(7)(C)	
	CSR 5.3.1	A list of critical applications, operations and data has been documented that: (1) prioritizes data and operations; (2) is approved by senior program managers; and (3) reflects current conditions.	164.308(a)(7)(ii)(E)	
	CSR 5.4.2	Backup files are created on a prescribed basis and rotated off-site often enough to avoid disruption if current files are lost or damaged.	164.308(a)(7)(ii)(A)	No requirement for rotation offsite
	CSR 5.4.4	The Contingency Plan specifies the critical data and how frequently they are backed up and details the method of delivery to and from the off-site security storage facility.	164.308(a)(7)(ii)(A) 164.310(d)(1)	

DRAFT Comparison of HIPAA to CMS Core Security Requirements (CMS CSR)

Category	CSR #	Control Technique	45 C.F.R. ____	Comments
Service Contini	CSR 5.4.5	A retrievable, exact copy of electronic CMS sensitive information exists before movement of equipment used to process such information.	164.310(d)(2)(iv)	
	CSR 5.5.1	Emergency processing priorities have been documented and approved by appropriate program and data processing managers.	164.308(a)(7)(ii)© 164.308(a)(7)(ii)(E)	
	CSR 5.6.2	Emergency procedures are documented.	164.308(a)(7) 164.310(a)(2)(i) 164.312(a)(2)(ii)	
	CSR 5.6.4	Emergency procedures are periodically tested.	164.308(a)(7)(ii)(D)	
	CSR 5.7.1	The current Contingency Plan is tested annually under conditions that simulate an emergency or a disaster.	164.308(a)(7)(ii)(D)	
	CSR 5.7.5	The Contingency Plan and related agreements are adjusted to correct any deficiencies identified during testing.	164.308(a)(7)(ii)(D)	
	CSR 5.12.1	The CMS Business Partner shall use special software to accomplish malicious software identification, detection, protection, and elimination.	164.308(a)(5)(ii)(B)	Not a complete match with HIPAA, and is only implied in the HIPAA training requirement

DRAFT Comparison of HIPAA to CMS Core Security Requirements (CMS CSR)

Category	CSR #	Control Technique	45 C.F.R. ____	Comments
Application Software and Change Control	CSR 6.3.13	All deposits and withdrawals of program tapes to/from the tape library are authorized and logged.	164.310(d)(2)(iii)	
	CSR 7.3.2	Each operator is required to use a unique password and identification code before being granted access to the system.	164.312(a)(2)(i)	HIPAA is more broadly applicable, not just to data entry operators
	7.3.3	When workstations are not in use, workstation rooms are locked and the workstations are capable of being secured.	164.310(c)	
	7.3.5	Each workstation automatically disconnects from the system when not used after a specific period of time.	164.312(a)(2)(iii)	
	7.3.6	Online access logs are maintained by the system and reviewed regularly for unauthorized access attempts.	164.312(b) 164.308(a)(I)(ii)(D)	
	CSR 10.1.1	An access list of personnel authorized to access a data center to process sensitive data is controlled.	164.310(a)(1)	
	CSR 10.1.2	Physical access to enclosures housing network equipment is restricted.	164.310(a)(2)(iii)	

DRAFT Comparison of HIPAA to CMS Core Security Requirements (CMS CSR)

Category	CSR #	Control Technique	45 C.F.R. ____	Comments
	10.2.1	Selected system elements at critical control points (e.g., servers and firewalls) provide logs of user network and system activity.	164.312(b)	
	10.2.2	Virus-scanning software is provided at critical entry points, such as remoteaccess servers and at each desktop system on the network.	164.308(a)(5)(i)(B)	Not a complete match with HIPPA, and is only implied in the HIPAA training requirement
	CSR 10.3.3	Policy exists identifying appropriate use of the E-mail system by employees, and procedures exist to enforce E-mail security, privacy, and message integrity	164.310(b)	
Network	CSR 10.4.1	Sensitive information being electronically transmitted must be protected. Two acceptable methods for transmitting sensitive information over telecommunications devices: (1) encryption and (2) guided media.	164.312(e)	
	CSR 10.4.2	Cryptographic tools have been implemented to protect the integrity and confidentiality of sensitive and critical data and software programs when no other means of protection exists.	164.312(a)(2)(iv) 164.312(c)	
	CSR 10.8.2	Authentication is used to: (1) restrict access to critical systems/business processes and highly sensitive data; (2) control remote access to networks; (3) grant access to the functions of critical network devices; (4) procedures for the above are documen	164.312(d)	
	10.9.1	A plan is in place to assess the risks to the network.	164.308(a)(1)(ii)(A)	

DRAFT Comparison of HIPAA to CMS Core Security Requirements (CMS CSR)

Category	CSR #	Control Technique	45 C.F.R. ____	Comments
	10.9.2	A plan is developed for eliminating significant vulnerabilities.	164.308(a)(1)(ii)(B)	
	10.9.3	A plan is developed for alerting, containing, and rebuffering a physical or cyber attack on the CMS Business Partner IS systems.	164.308(a)(6)	
	10.9.4	Assessments of the critical infrastructure's existing vulnerability, reliability, and threat environment are made at least annually.	164.306(e) 164.308(a)(8)	HIPAA does not have an annual requirement, just a periodic requirement