Medical Auditing Solutions LLC

APPLIES TO ALL HEALTHCARE & DENTAL PROVIDERS!

	Health Care Providers: Compliance & HIPAA/HITECH Checklist	Regulatory Section	Compliance	HIPAA	HITECH Security	Current Status
All security required 2009	**Assigned Responsibility to Manage (Compliance, Privacy, Security Officers) Required; Some companies may have a Regulatory Officer for all areas.**	Security 164.308 (a)(2)	**x**	**x**	**x**	
	Committee		**x**			
	Hotline or Direct Line for Reporting Concerns or Violations		**x**	**x**	**x**	
	Quarterly Committee Meetings include at least 1 C-level executive		**x**	**rec**	**rec**	
	Annual Independent Audit by Third Party Contractor		**x**	**x**	**x**	
	HITECH Security Policies & Procedures					
	Administrative Safeguards					
	Security Management Process					
1	**Implement policies and procedures to prevent, detect, contain, and correct security violations.**	164.308 (a)(1)			X	
	Risk analysis (Required)	164.308(a)(1)(ii)	x	x	x	
	Risk management (Required) to reduce risk	164.308(a)(1)(ii)	x	x	x	
	Sanction / Disciplinary Action policy (Required) for violators	164.308(a)(1)(ii)	x	x	x	
	Information system activity review (Required) such as audit logs, access reports, and security incident tracking reports.	164.308(a)(1)(ii)		x	x	
	Workforce Security					
3	Appropriate Workforce Access, Prevention & Termination	164.308(a)(3)		x	x	
	Information Access Management					
4	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.	164.308(a)(4)		x	x	
	Isolating health care clearinghouse functions (Required). The clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.	*164.308(a)(4)(ii)*		*x*	*x*	
	Access authorization, establishment, and modification (Addressable). Implement policies and procedures for granting & modifying access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.	164.308(a)(4)(ii)		x	x	

	Health Care Providers: Compliance & HIPAA/HITECH Checklist	Regulatory Section	Compliance	HIPAA	HITECH Security	Current Status
	Security Awareness and Training					
	Security & Malware Software (Addressable). Procedures for guarding against, detecting, and reporting malicious software.	164.308(a)(5)(ii)(B)			x	
	Log-in monitoring (Addressable). Procedures for monitoring log-in attempts and reporting discrepancies.	164.308(a)(5)(ii)(C)			x	
	Password management (Addressable). Procedures for creating, changing, and safeguarding passwords.	164.308(a)(5)(ii)(D)		x	x	
	Security Incident Procedures					
	Incident Response and reporting (Required) to suspected or known incidents	164.308(a)(6)(ii)	x	x	x	
	Contingency Plan					
7	Responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information. (Accreditation overlaps in some cases, check those policies if applicable to your business)	164.308(a)(7)			x	
	Data backup plan (Required).	164.308(a)(7)(ii)(A)			x	
	Disaster recovery plan (Required) to restore any loss of data.	164.308(a)(7)(ii)(B)			x	
	Emergency mode operation plan (Required) to continue critical business functions.	164.308(a)(7)(ii)(C)			x	
	Testing and revision procedures (Addressable) of contingency plans.	164.308(a)(7)(ii)(D)			x	
	Applications and data criticality analysis (Addressable). Assess the relative criticality of specific applications and data in support of other contingency plan components.	164.308(a)(7)(ii)(E)			x	
	Evaluation					

	Health Care Providers: Compliance & HIPAA/HITECH Checklist	Regulatory Section	Compliance	HIPAA	HITECH Security	Current Status
8	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. **(Required).**	164.308(a)(8)			x	
	Business Associate Contracts or Other Arrangements					
9	A covered entity, in accordance with Sec.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.	164.308(b)(1)		x	x	
	Physical Safeguards	164.310				
	Facility Access Controls Implementation Specifications	164.310(a)(2)				
	i) Contingency operations (Addressable). 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.				x	
	(ii) Facility security plan (Addressable). Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.				x	
	(iii) Access control and validation procedures (Addressable). 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.				X	
	(iv) Maintenance records (Addressable). Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).				X	
	Workstation Use	164.310(b)				

	Health Care Providers: Compliance & HIPAA/HITECH Checklist	Regulatory Section	Compliance	HIPAA	HITECH Security	Current Status
11	Implement policies and procedures that specify the proper 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 electronic protected health information. **(Required).**				x	
	Workstation Security	164.310 (c)				
12	Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.**(Required).**			x	x	
	Device and media controls receipt and removal of electronic PHI	164.310(d)(1)			x	
	(i) Disposal (Required). 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.	164.310(d)(2)			X	
	(ii) Media re-use (Required). Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re- use.				X	
	(iii) Accountability (Addressable). Maintain a record of the movements of hardware and electronic media and any person responsible therefore.				X	
	(iv) Data backup and storage (Addressable). Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.				X	
	Technical Safeguards	164.312				
	Access Control Implementation Specifications	164.312(a)(2)			x	
	(i) Unique user identification (Required). Assign a unique name and/or number for identifying and tracking user identity.			x	x	
	(ii) Emergency access procedure (Required). Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency. (Accreditation may over lap here)			x	x	
	(iii) Automatic logoff (Addressable). Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.			X	X	

	Health Care Providers: Compliance & HIPAA/HITECH Checklist	Regulatory Section	Compliance	HIPAA	HITECH Security	Current Status
	(iv) Encryption and decryption (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information.				X	
	Audit Controls	164.312(b)				
15	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information. **(Required)**				x	
	Integrity	164.312(c)(1)				
	Mechanism to authenticate electronic protected health information (Addressable). Policy & Procedure to Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner or electronically accessed, altered or destroyed in an unauthorized manner.				x	
	Person or entity authentication	164.312(d)				
17	Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. **(Required) Assigned based on Need to Know for job performance.**			x	x	
	Transmission Security measures to guard against unauthorized access to electronic protected health information	164.312(e)(1)				
	(i) Integrity controls (Addressable). Any modifications must be tracked to prevent unauthorized modification until time of destruction. (Duplicate of "Integrity" and can be built into that)			x	x	
	(ii) Encryption (Addressable). Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate. (Duplicate of item 95)				x	
	Business Associate & Other Contracts	164.314(a)(1)(2)				
	Business Associate contracts or other arrangements must extend responsibility of protection and violation; termination for failure to comply.	164.314(a)(1)		x	x	

	Health Care Providers: Compliance & HIPAA/HITECH Checklist	Regulatory Section	Compliance	HIPAA	HITECH Security	Current Status
	A) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the covered entity as required by this subpart;	164.314(a)(2)			x	
	(C) Report to the covered entity any security incident of which it becomes aware;	164.314(a)(2)(1)			x	
	Other Arrangements (when CE & BA are both governmental entities) (N/A 126-130 hidden)	164.314(a)(2)(ii)				
	Policies and Procedures and Documentation Requirements	164.316				
21	**(a) Standard: Policies and procedures. Implement reasonable** and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements.	164.316(a)(1)	x	x	x	
	(ii) All action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.	164.316(b)(1)	x	x	x	
	Implementation Specifications - Training and Revisions that effect any P& P or Company Standard	164.316(b)(2)	x	x	x	
	(i) Document Retention Time limit (Required). 6 years from the date of its creation or the date when it last was in effect, whichever is later. (This may be part of an existing Compliance or Privacy policy.)	164.316(b)(2)	x	x	x	
	Implementation of the Security Standards Deadline (Plans 2005, Clearinghouses 2006, Providers 2010)	164.318		x	x	
Compliance required 2007 or 2013, depending	**COMPLIANCE PROGRAM (Billing - Required by 2013) DRA required in 2007 for providers $5M+ in Medicaid collections collectively.**					
	Standards of Conduct					
	ANTIKICKBACK STATUTE		x			
	STARK LAW		x			
	AGENT/SERVICES COMPENSATION		x			
	AUDITING & MONITORING		x			

	Health Care Providers: Compliance & HIPAA/HITECH Checklist	Regulatory Section	Compliance	HIPAA	HITECH Security	Current Status
Billing Policies may not be all inclusive, due to specific issues by provider	BILLING: CLAIM FILING AND APPEALS		x			
	BILLING ASSIGNED CLAIMS		x			
	BILLING PATIENTS WITHOUT INSURANCE		x			
	BILLING: ONLY MEDICALLY NECESSARY SERVICES		x			
	BILLING: ORDERED AND PROVIDED		x			
	BILLING: DISCOUNTS		**x**			
	BILLING: PAST TIMELY FILING		x			
	DETAILED WRITTEN STATEMENT OF ORDERING PHYSICIAN		x			
	COMPLAINT TRACKING LOG		x			
	CONFLICT OF INTEREST		x			
	EXCLUDED PROVIDERS OR SANCTIONED PROVIDERS		x			
	LICENSURE & CREDENTIALING		x			
	INCENTIVES		x			
	INSURANCE VERIFICATION		x			
	INVESTIGATORS		x			
	MEDICAL RECORDS		x			
	MEDICARE SECONDARY PAYOR		x			
	NO UPCODING		x			
	PATIENT CONTACT - doesn't really apply, but we might discuss. Does Excel ever contact a patient?		x			
	PLACE OF SERVICE CODES		x			
	PROOF OF SERVICE		x			
	RECORD MAINTENANCE		x			
	REFUNDS & OVERPAYMENTS		x			
	RESPONDING TO BILLING AUDITS		x			
	RESUBMISSION OF CLAIMS		x			
	PROVIDER NUMBERS		x			
	ADVANCED NOTICE TO BILL PATIENTS ON POTENTIALLY DENIABLE CLAIMS		x			
	PROHIBITION ON REFUSAL TO SUBMIT A CLAIM TO MEDICARE		x			
	PROHIBITION ON UNBUNDLING ITEMS		x			

	Health Care Providers: Compliance & HIPAA/HITECH Checklist	Regulatory Section	Compliance	HIPAA	HITECH Security	Current Status
	WORKING PART-TIME FOR A POTENTIAL REFERRAL SOURCE		x			
	WRITE OFF OF REVENUE		x			
	ABUSE REPORTING		x			
	Acronyms		x	x	x	
	Modifiers		x			
Privacy required 2003	PRIVACY-NOTICE OF USE			x		
	PRIVACY-CONSENT			x		
	PRIVACY POLICY- MEDICAL RECORDS			x		
	PRIVACY- MEDICAL RECORDS CORRECTIONS			x		
	PRIVACY- De-identifying PHI			x		
	PRIVACY-MEDICAL RELEASE/AUTHORIZATION			x		
	PRIVACY-BUSINESS ASSOCIATES			x		
	PRIVACY-COMPUTER USE			x		
	PRIVACY-COMPLAINT PROCESS			x		
	PRIVACY-PENALTIES			x		
	RED FLAG RULE – IDENTITY THEFT			x		
	TRAINING OF 7 HOURS PER YEAR ON OIG TOPICS + HIPAA		x	x	x	