

HIPAA Security Standards Compliance Advisor

Summary of Requirements	Planning Questions	Yes	No
Administrative Safeguards: 164.308 (a) (1) <ul style="list-style-type: none"> · Procedures · Policy · Security Posture 	1) Have you implemented an Information System Activity review? 2) Have you implemented policies and procedures to prevent, detect, contact and correct security violations, focusing on: <ul style="list-style-type: none"> · Risk analysis · Risk management · Sanction policy 3) Have you begun to determine what products and services you will need for your security deployment?		
Administrative Safeguards: 164.308 (a) (2) 164.308 (a) (3) 164.308 (a) (4) 164.308 (a) (6) 164.308 (b) (1) 164.310 (b) 164.310 (c) 164.308 (d) (1) <ul style="list-style-type: none"> · Documentation of Procedures and Technology · Processes and Plan for Deployment 	1) Can you describe your level of importance for the following ISO- 17799 principles? <ul style="list-style-type: none"> · Confidentiality · Integrity · Availability 2) Have you assigned security responsibilities in your organization? 3) Have you implemented policies and procedures for authorizing information access and availability? 4) Have you documented all processes and procedures?		
Technical Safeguards: 164.312 (a) (1) 164.312 (b) 164.312 (c) 1164.312 (d) 164.312 (e) (1) 164.308 (a) (1) <ul style="list-style-type: none"> · Access Control · Audit Control · Information Integrity · Person or entity authorization · Transmission security 	1) Have you implemented technical systems that maintain electronic protected information to allow access only to these persons or software programs that have been granted access rights? 2) Have you implemented hardware, software and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information? 3) Have you implemented a mechanism to authenticate electronic protected information? 4) Have you implemented electronic mechanisms to corroborate that electronic protected information has not been altered and destroyed in an unauthorized manner? 5) Have you implemented technical security measures to guard against unauthorized access to electronic protected information that is being transmitted over an electronic communications network?		
Administrative Safeguards: 164.308 (a) (7) 164.308 (a) (8) <ul style="list-style-type: none"> · Testing and revision procedures · Contingency plans and procedures · Continual remediation of vulnerabilities 	1) Have you implemented policies and procedures to address security incidents, and a contingency plan to response to emergency situations? 2) Have you set a plan in place as how your organization will perform periodic technical evaluation in the future in response to environmental or operational changes affecting the security of electronic protected information? 3) Are you in need of 24/7 guaranteed Managed Security Services?		
Administrative Safeguards: 164.308 (a) (5) <ul style="list-style-type: none"> · Employee training · General security awareness and training 	1) Have you developed a training plan for your employees and business associates? 2) Would you like to receive periodic updates and security reminders?		