



DENTISTRY  
MSP

## PHYSICAL SITE AUDIT

Regulation	Description	Question	Yes	No
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a).	Are documents that contain Protected Health Information stored in boxes, under desks, on window sills, on desktops, or in other unlocked storage areas?		
164.308(a)(1)(ii)(A)	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.	Does your site store Protected Health Information at a long-term storage facility?		
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a).	Are documents with Protected Health Information left out on desktops at the close of business?		
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a).	Are documents with Protected Health Information left out on desktops at the close of business?		
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a).	Are documents with Protected Health Information stored in filing cabinets?		
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a).	Are filing cabinets locked each evening at the close of business?		
164.308(a)(1)(ii)(A)	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.	Do your employees send print jobs to printers located within a secured, supervised area?		
164.308(a)(1)(ii)(A)	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.	During your walk-through did you discover any documents on the printers waiting to be picked up?		

Regulation	Description	Question	Yes	No
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a).	Are the printers located in a common area or near a corridor through which visitors or staff from other sites often pass?		
164.308(a)(1)(ii)(A)	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.	Have the printers been checked for hard drives or other means of electronic storage?		
164.308(a)(1)(ii)(A)	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.	Do your employees use a fax machine within a secured or supervised area?		
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a).	During your walk-through were there any documents on the fax machine waiting to be picked up?		
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a).	Do your employees attend to the fax machine on a regular basis throughout the day?		
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a).	Is there evidence that your employees use a cover sheet when transmitting faxes?		
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a).	Do your employees dispose of documents that contain Protected Health Information in a proper manner (i.e. locked trash receptacle)?		
164.308(a)(1)(ii)(A)	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.	Did you observe documents with Protected Health Information in open wastebaskets or boxes under desks?		
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a).	Do you allow your employees to take documents or files containing Protected Health Information off-site or to work on at home?		
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a).	Do your employees follow proper procedures (i.e. discarding in locked shredder boxes) when dealing with documents that contain Protected Health Information like notepads, ringed binders, or scratch paper (particularly at the front desk)?		

Regulation	Description	Question	Yes	No
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a).	(For Covered Entities Only) Are patient interviews conducted in a secure room or secluded from other patients?		
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a).	Did you observe fire extinguishers at the site?		
164.308(a)(1)(ii)(A)	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.	(For Covered Entities Only) Are there any computers in the patient examination rooms?		
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a).	(For Covered Entities Only) If so, are the screens locked when an employee is not accessing the computer?		
164.308(a)(1)(ii)(A)	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.	Is your main server at a different location and is it secure?		
164.308(a)(1)(ii)(A)	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.	Are your servers that contain ePHI on-site and in a secure room?		
164.308(a)(1)(ii)(A)	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.	If your server is on-site, is it connected to the internet?		
164.308(a)(1)(ii)(A)	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.	If your server is on-site and connected to the internet, does it have a firewall?		
164.308(a)(1)(ii)(A)	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.	Does your network have a wireless router?		

Regulation	Description	Question	Yes	No
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a).	If you do have a wireless router, is encryption turned on?		
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a).	Is there anyone connecting to the server from home or other remote locations?		
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a).	Do all workstations in the office or at employees' homes (if you allow them to work from home) have antivirus software and the hard drive is encrypted on their computers?		
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a).	On the workstations that connect to ePHI, do you have the antivirus software automatically download any new virus definitions?		
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a).	On the workstations that connect to ePHI does your antivirus program run periodically and automatically?		
164.308(a)(1)(ii)(A)	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.	Do any of the individual workstations store ePHI (i.e. have PHI documents stored on them)?		
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a).	Have PC USB ports been disabled?		
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a).	When reviewing workstations, were they positioned so it would be difficult for non-employees to view the screen?		
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a).	Is your Network Closet (where your internet, phone system, and server are located) locked and secure at all times?		
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a).	Are employees in the habit of locking their workstations when leaving them for any amount of time, especially workstations in high traffic areas?		

Regulation	Description	Question	Yes	No
164.308(a)(1)(ii)(A)	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.	During the walk-through, did you observe an alarm system for the doors and windows?		
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a).	Was the alarm system in working order and have you tested it?		
164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a).	Was an emergency number readily available throughout the site in case of an emergency?		