HIPAA Inspection Checklist

TECHNICAL SAFEGAURDS SEC. 164.312 HIPAA Privacy Rule

Requirement	PASS	FAIL
1) The Computer's Operating System must be Windows NT 4.0, 2000 Pro, or XP.	_____	_____
2) Each Computer Workstation must have a unique username and password set.	_____	_____
3) Passwords should contain 8 or more characters, using both capital and lowercase letters as well as numbers or other characters like the # sign.	_____	_____
4) Servers must run on Windows NT4, NT4 Server, 2000 Pro, 2000 Server, XP Pro, Server 2003, UNIX or LINUX Professional Flavors, Mac OSX Server, or Novel Netware 4 or above.	_____	_____
5) All Microsoft Operating Systems, including Server Operating Systems, must be current on all Microsoft Critical Updates and Security Updates.	_____	_____
6) All database software (Lytec, Medisoft, ect.) that contains EPHI, there must be a unique username and password set, same as in requirements 2 and 3.	_____	_____
7) All EPHI software must have a timeout or auto log off procedure configured.	_____	_____
8) Access privileges on all user accounts must coincide with administrative documentation.	_____	_____
9) Servers must have audits set and configured for monitoring all accounts logon and off.	_____	_____
10) Email software must support 128-bit encryption, such as OE 2k Pro or OE Exp 6	_____	_____
11) All emails sent containing EPHI must be sent encrypted.	_____	_____
12) All EPHI databases must on a secure backup system.	_____	_____
13) Backup system must include secure, HIPAA compliant off-site data storage AND a redundant database onsite, such as a RAID mirror on the server.	_____	_____
14) Firewalls are required if computer systems are hocked up to broadband Internet connection.	_____	_____
15) Firewalls must internally log port scans.	_____	_____
16) Firewalls must contain a unique username and password set, same as in requirements 2 and 3.	_____	_____
17) All VPN tunnels, if present, must contain a secure encryption level.	_____	_____
18) All EPHI software must be HIPAA compliant.	_____	_____

ADMINISTATIVE SAFEGAURDS SEC. 164.308 HIPAA Privacy Rule

All Providers must keep a detailed administrative log of the following:	Pass	Fail
1) Detailed list of all usernames and passwords for all workstations and email accounts.	_____	_____
2) Detailed list of all usernames and passwords for all EPHI database software	_____	_____
3) Detailed list of all usernames and passwords for all Servers and database server software	_____	_____
4) Detailed list of all usernames and passwords for all router and firewall equipment	_____	_____
5) Detailed list of user privileges for all employee's user accounts on all workstations	_____	_____
6) Detailed list of user privileges for all employee's user accounts in all EPHI database software	_____	_____
7) Detailed list of user privileges for all accounts in server, including all network accounts in the active directory (Windows 2000 Server)	_____	_____
8) All user privilege lists need to shy WHY employees have access (ex, Tina Smith is a surgery scheduler, and had full access to EPHI database records, but cannot change them)	_____	_____
9) Log of employees who have full administrative rights to workstations, servers, EPHI databases, routers, firewalls.	_____	_____
10) Log of employees who have access to server rooms, or any other location where EPHI is stored.	_____	_____
11) Detailed list of daily backup procedures and who is in charge of them	_____	_____
12) Log of all employees who store data backup tapes offsite	_____	_____
13) Log of any other person(s) or company (if applicable) who store EPHI offsite	_____	_____
14) List of all employees who handle Direct Data Entry	_____	_____
15) List of all employees who have access to ANY EPHI	_____	_____
16) Medicare claims cannot be sent using J codes; only NCD codes.	_____	_____
17) Record of any security incidents and their outcomes	_____	_____
18) Data contingency plan should be documented, and include where all offsite EPHI is stored, a procedure for what to do if Server data fails, and how data will be restored.	_____	_____

All above information should be stored with the Practice HIPAA Policy and Procedure Manuel where only Doctors, Office Managers, and IT administrators (with BA contracts if not employed by the provider) have access. A copy may also be kept in a HIPAA compliant attorney's office.

TERMINATION PROCEDURE (ADMINISTRATIVE, SEC. 164.308) HIPAA Privacy Rule

Provider should have list included with other administrative documentation, which include the following:

	Pass	Fail
1) All former employees with their names, position, and when they left the practice.	_____	_____
2) Change of ALL of the former employees usernames and passwords.	_____	_____
3) All documents and email data of any kind must be removed from the former employee's workstation AND archived on secure store media.	_____	_____

CHAIN OF TRUST AGREEMENTS (BUSINESS ACCOCIATE CONTRACTS) ADMINISTRATIVE SAFEGAURDS SEC. 163.308 HIPAA Privacy Rule

1) Presence of BA Contract with all person(s) who have access to EPTI	_____	_____
a) Contract has to have the following:	_____	_____
a. Background and Purpose		
b. Privacy Rule Definitions	_____	_____
c. Obligations of the Parties with Respect to PHI	_____	_____
d. Termination Clause; if Contract Holder is not HIPAA compliant, or violates any HIPAA rules or Practice rules, then those violations must be documented, and they can be terminated at the will of the Practice.	_____	_____

HIPAA EMPLOYEE AWARENESS TRAINING, ADMINISTRATIVE SAFEGAURDS SEC. 163.308 HIPAA Privacy Rule

1) Provider must have a staff training procedure in affect.	_____	_____
2) Training Procedure must include:		
a. General HIPAA information		
b. Compliency dates		
c. All HIPAA procedures that pertain to the induvidual employee's day to day work.	_____	_____
d. Documentation of when the employee completed HIPAA training	_____	_____
e. All employee's must be updated when new HIPAA procedures are added onto the practice's HIPAA policy, or when new HIPAA amendments are added onto the Privacy Rule by HHS.	_____	_____
f. Provider must then re-train employees on all NEW procedures.	_____	_____
g. All employee re-training must be documented	_____	_____
h. All new employee's must be trained within a reasonable amount of time after they are hired.	_____	_____

LOCAL PRIVACY RULE MANUAL, ADMINISTRATIVE SAFEGAURDS SEC. 163.308, HIPAA Privacy Rule

1) Provider must have ON HAND a manual explaining all of their local procedures pertaining to HIPAA compliency, which must explain IN DETAIL EVERY procedure done to enforce and ensure HIPAA compliency. _____ _____

PHYSICAL SAFEGAURDS SEC. 164.310, HIPAA Privacy Rule

1) Operational access control procedure for all staff and visitors in place _____ _____

2) All paper PHI is in an area accessable only to authorizes staff, or is watched by authorized staff at all times. _____ _____

3) Local Privacy procedure includes that all paper PHI storage units are locked during non-business hours or lunch hours UNLESS there is an authorized employee who will be in the area to ensure their security. _____ _____

4) All EPHI storage rooms, such as server rooms must be LOCKED AT ALL TIMES _____ _____

5) All EPHI storage rooms, such as server rooms, must have a document logging all personal who enter the room, including the times the entered and exited, and this this list should be stored IN the LOCKED ROOM. _____ _____

6) Restrected Access sighs need to be posted in any area containing PHI in ANY form (Server Rooms, Rooms containing patient charts, ect). _____ _____

Geomar Computers
Technology for today's world

www.GeomarComputers.com/hipaa
hipaa@geomarcomputers.com

Geomar Computers
5980 Fairmount Avenue Suite 111
San Diego, CA 92120
619-283-2364