Sample HIPAA Compliance Checklist

Using an EMR (electronic medical records) program can help your organization maintain HIPAA compliance: for example, PIMSY has an automatic log-off feature that can be set to your specifications. PIMSY also offers security profiles so you can control exactly what staff members can see and do within the system and give them access only to certain records.

Regardless of what PIMSY provides, practices should *always* conduct company and system wide HIPAA compliance testing and training to ensure that compliance is maintained. This sample checklist provides a good idea of things to consider:

		Y	N	Notes/Observations
1	Is there PHI (protected health information) in the regular trash bins?			
2	Are shred containers or other PHI disposal bins easily accessible by staff members?			
3	Are shred containers kept locked?			
4	Are documents to be shredded left in the open, including overnight?			
5	Are documents containing PHI (appointment schedules, lab orders, client invoices) visible to unauthorized individuals, including the general public?			
6	Are documents containing PHI left in unattended areas?			
7	Are client charts maintained and stored in a secure area?			
8	Are materials removed from printers and fax machines in a timely manner? Are the machines checked at night? Are unclaimed documents stored in a secure manner and location?			
9	Do staff members verify fax numbers before sending a fax?			
10	Are staff members restricted within electronic records to only have access to PHI for which they are approved? (PIMSY lets you set any desired parameters via security profiles)			
11	Have all staff and faculty completed HIPAA training?			
12	Do staff members ensure that all conversations containing PHI are necessary and the minimum amount of PHI possible is discussed?			
13	Do staff members ensure that all necessary conversations containing PHI are kept private and out of earshot of unauthorized individuals?			
14	Is there a process for identifying and issuing clients who need to receive a Notice of Privacy Practices (NPP) and for collecting & documenting the client's signed acknowledgement of receiving the NPP?			

		Y	N	Notes/Observations
15	Do staff members log-off computers before leaving their workstations? (PIMSY has auto-log off that can be set to desired time-out specifications.)			
16	Are computer monitors and printers located in secure areas, and are they positioned so that the public can't access or view PHI on them?			
17	Do staff members protect their hardware and/or software logins and make sure they are not accessible at their workstations or by unauthorized individuals?			
18	Do staff members make sure they're not sharing another employee's login to hardware and/or software?			
19	Can clients in the waiting room overhear the registration process?			
20	Do clients or the public have access to any areas in the building where confidential information is stored or accessible?			
21	Do staff members know that they should not access the health information of their co-workers, family or friends?			
22	Do staff members know what to do if clients request amendments to their records/chart?			
23	Do staff members know what to do if clients request their records/chart?			
24	Do staff members know who to contact if they have questions about HIPAA and/or client privacy (ie, Chief Compliance Officer and Privacy Director)?			
25	Do staff members know where they should refer questions regarding HIPAA and/or client privacy?			
26	Are staff members making sure they don't use the preview pane when viewing emails?			
27	Are checks and cash locked up overnight?			
28	Are computers and scanners shut down completely at the end of the day?			
29	Are privacy/confidentiality/security signs posted for the custodial staff?			
30	Are security doors (file room, office) locked and operational?			

Some additional easy HIPAA compliance ideas to consider:

- a fax cover page that goes out with all documents letting the recipients know that the information being sent is confidential and needs to be handled under HIPAA privacy guidelines.
- "remember to log off" stickers placed at every workstation to remind staff members to restrict access to any confidential materials before leaving their desks.

PIMSY
Provider Information Management Systems