HIPAA Privacy Self-Assessment Checklist

Clinic Name:			
Name of Reviewer:		Review Date:	

Item	Item	Yes	No	Documentation/Observations
1	Is there PHI in the trash receptacles?			
2	Are shred containers or other PHI disposal bins available and easily accessible by staff members?			
3	Are documents containing PHI (e.g. appointment schedules, census lists, physician orders) visible to unauthorized individuals – including the public			
4	Are patient charts maintained/stored in a secure area?			
5	Are materials removed from printers and fax machines in a timely manner?			
6	Have all staff and physicians completed HIPAA training and is the training documented?			
7	Does the location have a process for identifying and issuing patients who need to receive a Notice of Privacy Practices (NPP) and for collecting and documenting the patient's signed acknowledgment of receiving the NPP?			
8	Do physicians/staff log-off computers before leaving their workstations?			
9	Are computer monitors and printers located in secure areas, and are they positioned so that visitors can't access or view the PHI on them?			
10	Do staff members verify fax numbers prior to use?			
11	Can visitors in the waiting rooms overhear the registration process?			
12	Are physician/staff aware that they should only access PHI that they need to know to perform their work related duties?			
13	Do physician/staff know that they should specifically not access their co-workers, supervisor, family, friends, and their own information?			
14	Do physician/staff know what to do when patients request their medical records?			
15	Do physician/staff know what to do if patient request amendments to their medical records?			
16	Do physician/staff know where they should refer questions regarding patient privacy?			
17	Do physician/staff log-off when they leave their workstation/computer?			
18	Does the location have a whiteboard, patient tracker (electronic), or other posting mechanism that contains only the minimum amount of information necessary and is it located in a secure area (staff only or quasi-public area)?			