HIPAA SECURITY ABBREVIATED RISK ASSESSMENT CHECKLIST

For the office of: _____

Date: _____ Inspected by: _____

Have you kept an updated inventory of hardware and software owned by the practice? (See Form 7-Inventory Log in the back of your HIPAA Security manual)			
Can you identify where ePHI is located (desktops, laptops, handhelds, tablets, removable media, servers, etc.)?			
Could you locate the inventory log in a disaster (fire, flood, explosion, theft)?			
Do you know the current approximate value of your hardware and software?			
Do you have an Emergency Contact List completed with information for workforce members and service providers?			
Who's responsible for modifying user access and assigning passwords? Does access correspond to job descriptions (clinical, administrative, billing)? Are passwords changed on a regular basis? Have you established procedures for assigning, changing, and safeguarding passwords?			
Do you or any employee take home portable computers or other devices that contain ePHI? Are employees with laptops, PDAs, or cell phones aware of encryption requirements?			
Have vendors that have access to protected health information signed a current Business Associate Agreement?			
Has initial training for all new hires and continuing training being documented? *Training records must be kept for 6 years.*			
Have you implemented sanctions in your policies against employees who do not abide by your policies? Have employees been made aware and are you enforcing these sanctions?			
Have audit controls been set up to monitor system activity? Do you review these audit logs for inappropriate use or activity by an employee? Are you notified of unsuccessful log-ins? Are log in attempts limited to a certain number of tries and does your software monitor log in attempts?			
Do you immediately deactivate an employee's access upon termination or upon change of job description? (See Form 14-Termination Form in the back if the Security manual)			
HIPAA Security requires periodic security reminders for staff. Has this been implemented? (You can always post Oshaguard's Guardian Newsletter)			
Do employees know the location of your HIPAA Privacy and Security Policies?			
Have you installed anti-virus and other anti-malware protection software on your computers? Do you use it to guard against, detect, and report any malicious software?			
Are employees prohibited from bringing software or downloading games, data, etc. unless authorized to do so? *The use of unauthorized software must result in penalties under your Sanction Policy.*			
Have employees been training to report all security incidents to their Security Officer immediately?			
Are policies in place and a Maintenance Log *(must be kept for 6 years)* documenting repairs to physical components related to security? (doors, locks, hardware, alarms, keys, etc.)			
Are appropriate policies in place for damaging or erasing data on hardware of electronic media prior to disposal? Copier, fax machine, hard drives?			
Do your computers automatically log off after a specific period of inactivity?			
	YES	NO	N/A

HIPAA SECURITY ABBREVIATED RISK ASSESSMENT CHECKLIST

In order to comply with HIPAA, you'll need to take the following corrective actions:

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____