Sharon's Quick & Dirty HIPAA Privacy & Security Checklist	Y/N
1. Does your organization ensure that its risk management program restricts the impermissible use and disclosure of PHI?	
2. Has your organization developed, documented, and implemented policies and procedures for assessing and managing risk for all forms of PHI?	
3. Does your organization have policies and procedures that authorize members of your workforce to have access to PHI and describe the types of access that are permitted?	
4. Does your organization have formal policies and policies and procedures to support when a workforce member's employment is terminated and/or a relationship with a business associate is terminated?	
5. Does your organization have policies and procedures for contingency plans to provide access to PHI to continue operations after a natural or human-made disaster?	
6. Does your organization have an emergency mode operations plan to ensure the continuation of critical business processes that must occur to protect the availability and security of PHI immediately after a crisis situation?	
7. Does your organization have senior-level personnel responsible to develop and implement pricavy/security policies and procedures? Do these staff have responsibility to decide who can access PHI (and under what conditions) and to create PHI access rules that others can follow?	
8. Does your organization have a training program that requires that each board member/staff/volunteer (including temporary/contingent staff) with access to PHI is trained on privacy/security measures to reduce the risk of improper access, uses, and disclosures?	
9. Does your organization keep records that detail when board/member/staff/volunteers satisfactorily completed periodic training?	
10. Does your organization maintain a list of all of its subcontracted network, idenrtifying which of them have access to your organization's facilities, information systems and PHI?	
11. Do you execute a BAA (or similar document) with your subcontracted networks that use/disclose PHI to transact business on your behalf requiring them to follow Privacy/Security regulations? How do you verify compliance?	
12. Do your subcontracted network Agreements include provisions for immediate reporting of privacy/security breaches to your organization?	
13. Does your organization have policies and procedures that describe how to position workstations to limit the ability of unauthorized individuals to view PHI?	
14. Does your organization maintain a record of use/locations of hardware and media and the staff responsible for the use and security of the devices or media containing PHI use offsite?	