Periodic Security Evaluation Checklist

(The Security Officer should complete this form every time that a periodic evaluation is completed – copies should be made of this form to use for each evaluation)

Date of Evaluation: _____

	Requirement	Policy / Procedure Reference	Yes/No	If No, steps that will be taken to achieve/enhance compliance
1	Has a Security Officer been designated and is the decision documented?	Explanation of Policy 1		
2	Is the Risk Analysis up to date (Have systems/conditions changed since last risk analysis?) and are Worksheets 1, 2 and 3 up to date?	Policy 1 - Section 1, Procedures 1& 2; Worksheets 1, 2 & 3		
3	If risks have been identified, have safeguards been implemented to mitigate those risks through a cost-benefit analysis?	Policy 1 – Section 2, Procedure 3		
4	Is the organization disciplining employees who breach HIPAA Security Policies and Procedures in compliance with the Policy 1 and the organization's disciplinary policies?	Policy 1 - Section 3, Procedure 4		
5	Is the information system activity review being performed in accordance with the schedule set by the Security Officer (as documented)?	Policy 1 - Section 4, Procedure 6		
6	Are you satisfied that all necessary reports are being run during the information system activity review schedule, or that the frequency of reports is appropriate?	Policy 1 - Section 4, Procedure 5		

7	Are all reports that are being run as part of information system activity review being retained in accordance with Policy 1?	Policy 1 - Section 4, Procedure 6		
8	Are investigations being conducted and documented when the information system activity review identifies suspicious activity?	Policy 1 - Section 4, Procedure 7		
9	Are unauthorized members of the workforce being supervised in accordance with Policy 2?	Policy 2 - Section 1, Procedure 2		
10	Are workforce clearance procedures being followed in accordance with Policy 2 for individuals who have access to electronic protected health information?	Policy 2 – Section 2, Procedure 3; Form 2.1		
11	Are all termination procedures, (such as password deletion, return of keys, etc.) being followed in accordance with policy 2?	Policy 2 – Section 3, Procedure 4		
12	Has a determination as to the level of password protection needed for various members of the workforce been made?	Policy 3 – Section 1, Procedure 1		
13	Has a determination been made and documented regarding which members of the workforce should have access to electronic protected health information, and what their respective levels of access should be? Is this determination up to date?	Policy 3 – Section 2, Procedure 2; Form 3.1		
14	Are employees being provided periodic security reminders in accordance with Policy 4?	Policy 4 – Section 1, Procedure 1		
15	Are employees being trained on virus (and other malicious software) protection and prevention, login monitoring, and password management in	Policy 4 – Section 2, Procedure 2		

	accordance with Policy 4?			
16	Are employees complying with the log-in monitoring and password management policies in accordance with Policy 4?	Policy 4 – Sections 3 & 4, Procedures 3 & 4		
17	Are security incidents being reported and documented in accordance with Policy 5?	Policy 5 – Sections 1 & 2, Procedures 1 & 2		
18	For any security incidents that have occurred, have mitigating steps been taken and has documentation of such steps been retained in accordance with Policy 5?	Policy 5 – Section 3, Procedure 3		
19	For any security incidents that have occurred, have appropriate notifications been made in accordance with Policy 5?	Policy 5 – Section 4, Procedure 4		
20	Has the applications and data criticality analysis been performed in accordance with Policy 6?	Policy 6 – Section 1		
21	Have the data backup, disaster recovery, and emergency mode operation plans been created and adhered to in accordance with Policy 6	Policy 6 – Sections 2 & 3		
22	Have the contingency plans been tested in accordance with Policy 6?	Policy 6 – Section 4		
23	Have the Security Policies and Procedures been periodically evaluated, and have such evaluations been documented, in accordance with Policy 7?	Policy 7 – Section 1, Procedures 1 - 3		
24	Have all business associates who have access to, maintain, or create electronic protected health information been asked to sign a business associate agreement with the additional language required by the Security Rule?			
25	Has access to the facility been	Policy 8 –		

	determined by the Security Officer (e.g., who has access after hours or to equipment rooms) and are unauthorized individuals being prohibited from gaining access in accordance with Policy 8?	Sections 1 & 2		
26	Have visitor control policies been implemented and are they being complied with in accordance with Policy 8?	Policy 8 – Section 3		
27	Is a maintenance log being kept in accordance with Policy 8?	Policy 8 – Section 4		
28	Are workstations being protected from unauthorized access and from destruction in accordance with Policy 9?	Policy 9		
29	Are hardware, electronic devices and media being properly erased prior to reuse and erased or destroyed prior to disposal in accordance with Policy 10?	Policy 10 – Procedures 1 & 2		
30	Are exact duplicate copies being made of protected health information prior to moving or erasing such information that is stored on hardware in accordance with Policy 10?	Policy 10 – Procedure 3		
31	If hardware or electronic media is moved, is documentation maintained in accordance with Policy 10?	Policy 10 – Procedure 4		

Security Evaluation Checklist Explanation

As discussed in Policy 7 regarding the Evaluation Standard and its associated Explanation, the HIPAA Security Rule requires covered entities to periodically perform an evaluation of both technical and non-technical security safeguards to determine whether the covered entity is in compliance with the Security Rule. The evaluation should be done, not only periodically, but also in response to any operational or environmental changes that could impact the original analysis (for example, a move to electronic health records from paper records would warrant a reevaluation of HIPAA Security compliance).

The enclosed Periodic Security Evaluation Checklist is one tool that could be used to evaluate your practice's compliance efforts on a periodic basis. The checklist, or other tool that is used to assess compliance, should be retained for at least six years.