HIPAA Documentation Requirements Checklist

Department: _____ Date: _____

Name: _____

System/Application: _____

The following security process and procedure controls must be documented for any system which handles HIPAA personally identifiable health information, classified as Level III (restricted) data.

___1. Perform and document a **risk assessment** for the system annually. This includes identification of assets, identification of the risks to those assets, and procedures to mitigate those risks.

___2. Describe the criteria used for **account eligibility**, and the procedures for determining access duration and expiration. Also describe how **account privileges are reviewed**, including the interval between reviews and the responsible party. Also, describe the procedures (approval, follow up, oversight) to be used in the event that **emergency access to the system** is necessary.

___3. Describe procedures used to **review audit records** (e.g., user activity records, transaction logs, system error messages), and the procedures to respond to unusual or unexplained activity, including the interval between reviews and the responsible party.

___4. Describe how **employee terminations** are handled and the process by which you are made aware of employee terminations, and what steps are taken (attach termination checklist if applicable).

___5. Document the **change control procedures** used for systematic review and approval of all changes to hardware and software of the named system. (Request, approval, testing, implementation, and reporting.)

___6. Describe the **system backup procedures**. Include the method for producing backups, and the frequency of backups. Document the restoration process/procedures used for both limited/partial failures and a full system failure. Specify the off-site storage location used for backups, and the process for utilizing it.

___7. Document a **Disaster Recovery Plan**. It must include the following elements:

A.) **Contact Information** for business owner(s), and the person(s) involved with support of the system, including after-hours information.
B.) **Prioritization of Recovery** for all systems, processes, and data.
C.) **Emergency Operations Procedures**. This may include use of an alternate system, using manual procedures, or another method of accomplishing the system purpose. Include the duration of outage that can be tolerated before emergency operations procedures must be invoked.
D.) **System Recovery Procedures**. Provide detailed steps, and resources needed to recover the system, including sequences that support the recovery prioritization.

Feb. 2014

HIPAA Documentation Requirements Checklist

___8. Obtain and file signed **confidentiality agreements** from all individuals with privileged access to the system, as well as documented results of criminal background checks. Also keep records of the **security awareness training** and **HIPAA privacy training** for persons who support and/or use the system.

___9. Describe the **physical security** controls for the facility that houses the system. Include access control mechanisms, visitor control, and maintenance records, as well as the process for equipment/inventory control.

___10. Describe the **network security** controls which promote information privacy and integrity of the information while it's in transit.