**HIPAA Security, Privacy and Breach Notification Training**

It is the policy of [Insert Business Associate or Covered Entity Name] that all employees will access, use and disclose PHI only as permitted under HIPAA, and that all employees shall be vigilant with respect to guarding PHI. However, in the event that a potential breach of unsecured PHI occurs, the following policies and procedures shall be followed.

**What is a breach?**

A breach is any unauthorized acquisition, access, use, or disclosure of PHI that compromises the security or privacy of such information. A breach may involve PHI in any form, paper or electronic. “Compromises the security and privacy” of PHI means “poses a significant risk of financial, reputational, or other harm to the individual.” Any exceptions to this definition will be determined through the investigation and response process.

**Examples of a Breach:**

1. A hospital billing department sends a bill to the wrong individual which is opened by the recipient.

2. Lost or stolen laptops or PDA.

3. Losing a medical record.

4. An employee snooping in a patient’s file.

5. A clinic mails lab results to the wrong patient.

6. A hospital employee who is not authorized to access protected health information decides to look through patient files in order to learn of a friend’s treatment.

7. A briefcase containing patient charts is stolen from a health care provider’s car.

8. A hospital employee accidentally gives a discharge order form to the wrong patient.

9. A reminder notice for an appointment at an infectious disease physician’s office is mailed to the wrong address.

10. A Fax containing PHI is received from another organization in error.

11. A Fax containing PHI is sent to another organization in error.

**A. Step 1 – DISCOVERY**

A breach of PHI will be deemed “discovered” as of the first day an [Insert Business Associate or Covered Entity Name] employee becomes aware of the breach or, by exercising reasonable diligence, would or should have known about the breach. If a potential breach is discovered, it is very time sensitive and must be immediately reported to the Privacy Officer.

**B. Step 2 – INTERNAL REPORTING**

If you believe that a potential breach of PHI has occurred, you must immediately notify the Privacy Officer.

Please provide all of the information you have available to you regarding the potential breach, including names, dates, the nature of the PHI potentially breached, the manner of the disclosure (fax, email, mail, verbal), all employees involved, the recipient, all other persons with knowledge, and any associated written or electronic documentation that may exist. Notification and associated documentation may itself contain PHI and should only be given to the Privacy Officer. Please do not discuss the potential breach with anyone else, and do not attempt to conduct an investigation. These tasks will be performed by the Privacy Officer.

**C. Step 3 – INVESTIGATION**

Upon receipt of notification of a potential breach the Privacy Officer, or his/her designee, shall promptly conduct an investigation. The investigation shall include interviewing employees involved, collecting written documentation, and completing all appropriate documentation. The Privacy Officer shall retain all documentation related to potential breach investigations for a minimum of six years.

[Insert Business Associate or Covered Entity Name] employees who fail to fully comply with [Insert Business Associate or Covered Entity Name] HIPAA Privacy, Security and Breach Notification Policies and Procedures will be subject to sanctions as deemed appropriate by management in accordance with [Insert Business Associate or Covered Entity Name] employee policies and guidelines.

Employee\Volunteer Name: Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Employee\Volunteer Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[Insert Business Associate or Covered Entity Name] Security/Privacy Officer: **Management Team**