HIPAA Security Policy #6

Administrative Safeguards
Privacy and Security Incident Procedures

Statement of Policy

The Company is a *Business Associate* under the Health Insurance Portability and Accountability Act (HIPAA) Security Regulations. As such, The Company is required to safeguard electronic protected health information (ePHI) in accordance with the HIPAA Security Rule Regulations as well as The Health Information Technology for Economic and Clinical Health Act (the "HITECH Act"). These policies reflect The Company's commitment to complying with such Regulations. The Company will comply with the *Covered Entity's* documented HIPAA policies and procedures unless specifically stated in the below policy.

Purpose of Policy

The purpose of the policy is to develop the response to and reporting of security incidents, including the identification of and response to suspected or known security incidents, the mitigation of the harmful effects of known security incidents, to the extent possible, and the documentation of security incidents and their outcomes.

Policy

6 Privacy and Security Incident Procedures

TYPE: Standard
REFERENCE: 45 CFR 164.308(a)(6)(i)
SECURITY REGULATION STANDARDS LANGUAGE:
"Implement policies and procedures to address security incidents."

1. The Company will develop and document a procedure for identifying, responding to and reporting of all privacy and security incidents against ePHI or other critical systems.

6.1 Reporting and Response

IMPLEMENTATION TYPE: Required
REFERENCE: 45 CFR 164.308(a)(6)(ii)
SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:
"Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes."

1. The Company acknowledges that under The Health Information Technology for Economic and Clinical Health Act (the "HITECH Act") it is required to protect ePHI in the same regard as a covered entity.

2. The Company will ensure that all incidents, threats, or violations that affect or may affect the privacy, confidentiality, integrity, or availability of ePHI will be reported and responded to.

3. The Company shall have a Privacy and Security Incident Response Team ("IRT") charged with the responsibility of identifying, evaluating and responding to privacy and security incidents. The HIPAA Privacy and Security Officers shall oversee the activities of the IRT.

Procedure

1. The Company's IRT will be responsible for investigating all known or suspected privacy and security incidents to systems containing ePHI or other critical systems.

2. The Company will document a procedure for all workforce members to follow to report security incidents. See **Appendix A – Security Incident Response Log.**

3. The Company will ensure that all workforce members receive training on how to identify and report privacy and security incidents.

4. All workforce members must follow the documented procedure to report privacy and security incidents. In addition, workforce members must report all known or suspected privacy and security incidents.

5. All workforce members must assist the IRT with any privacy or security incident investigations.

6.2 Breach Determination

The Privacy and Security Incident Response Teams (IRT) will investigate all reported and suspected privacy and security breaches. The following guidelines will help determine if a privacy or security incident would be considered a breach as defined by the HIPAA Privacy, Security and Omnibus rules:

1. An acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Privacy or Security rules is presumed to be a breach unless The Company or a business associate demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

    i. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

    ii. The unauthorized person who used the protected health information or to whom the disclosure was made;

    iii. Whether the protected health information was actually acquired or viewed; and

    iv. The extent to which the risk to the PHI has been mitigated.

6.3 Breach Notification

Following the discovery of a breach of unsecured PHI, The Company will notify each individual whose unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, used, or disclosed as a result of such breach.

I. Date of discovery

A breach will be treated as discovered as of the first day the breach is known or by exercising reasonable diligence would have been known.

II. Timeliness of notification

The Company will provide the required notifications without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.

III. Content of notification

A notification will be provided to each individual affected by the discovered breach. The notification should include the following:

- A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
- A description of the types of unsecured PHI that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);
- Any steps patients should take to protect themselves from potential harm resulting from the breach;
- A brief description of what The Company is doing to investigate the breach, to mitigate harm to patients, and to protect against any further breaches; and
- Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.
- The notification should be written in plain language.

IV. Methods of notification

The following methods should be used to notify individuals affected by the discovered breach:

i. Written notice

Written notification by first-class mail to the patient at the last known address of the individual or, via e-mail if the patient agrees to e-mail notice. The notification may be provided in one or more mailings as information is available.

If the patient is deceased notifications will be sent to next of kin or personal representative

ii. Substitute notice

If contact information is out of date and written notification cannot be made, a substitute notification can be used.

- If contact information is out of date for fewer than 10 individuals, the substitute notification may be provided by an alternative form of written notice, telephone, or other means.

- If contact information is out of date for more than 10 individuals, the substitute notification may be in the form of either a conspicuous posting for a period of 90 days on the home page of The Company's Web site, or conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside. The notice should include a toll-free contact phone number that remains active for at least 90 days.

- In any case deemed to require urgency because of possible imminent misuse of unsecured PHI, notification may provide to individuals by telephone or other means, as appropriate, in addition to notice defined above.

V. Notification to media

In addition to notifying individuals of a known breach, a notification to the media is required if the breach involves more than 500 residents of a State or jurisdiction. The notification should occur no later than 60 days after the breach discovery.

VI. Notification to Health and Human Services (HHS)

The Company will notify HHS of a discovery of a known breach. The timing of the notification will be the following:

- For breaches involving 500 or more individuals a notification to HHS will occur no later than 60 days after the date of discovery.

- For breaches involving fewer than 500 individuals a notification to HHS will occur no later than 60 days after the end of each calendar year. All breaches involving fewer than 500 individuals in the calendar year will be reported to HHS 60 days after the end of each calendar year.

HHS has given guidance to breach notification on their website:
http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/

VII. Notification by business associates

Breaches discovered by business associates will be reported to a covered entity without delay and no later than 60 calendar days after discovery of the breach.

Creation Date:
Effective Date:
Last Revision Date:

Appendix A – Security Incident Response Log

Incident Identification Information	
Name:	
Phone:	‘
Email:	
Date/Time Detected:	
System / Application Affected:	
Incident Summary	
Type of Incident Detected: (Denial of Service, Malicious Code, Unauthorized Access, Unauthorized Use / Disclosure, Unplanned System Downtime, Other)	
Description of Incident:	
Names of Others Involved:	
Incident Notification	
How Was This Notified? (Security Office, IT Personnel, Human Resources, Other)	
Response Actions **Include Start and Stop times**	
Identification Measures (Incident Verified, Accessed, Options Evaluated):	
Containment Measures:	
Evidence Collected (Systems Logs, etc.):	