SECURITY POLICY
Administrative Safeguards:
Security Incident Procedures

I. Policy Statement

Prominic.NET is committed to conducting business in compliance with all applicable laws, regulations and policies. Prominic.NET has adopted this policy to provide guidance in the event of a breach of unsecured PHI or other security incident, and to identify steps that will be taken to contain the breach or security incident, conduct an investigation, mitigate damage and create proper documentation.

II. Required Legal Standard

In its capacity as a business associate, Prominic.NET must implement policies and procedures to address security incidents (45 CFR §164.308(a)(6)(i)). This standard includes the requirement for Prominic.NET to implement specifications for response and reporting of security incidents:

(1) 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 or business associate; and document security incidents and their outcomes (45 CFR §164.308(a)(6)(ii)).

III. Implementation Specifications

A. **Application:** This policy applies to all Prominic.NET workforce members.

B. **Scope of Policy:** This policy documents the policies and procedures for responding to a breach of unsecured PHI or any other security incident.

C. **Security Incident Response and Reporting (Required):** Prominic.NET has implemented a response and reporting system to report, mitigate, and document security incidents and violations.

1. Prominic.NET will exercise reasonable diligence to discover any potential breach.

2. Upon discovery of a potential breach or other security incident the workforce member will take immediate action to neutralize the threat.

3. Workforce member will notify the security officer of the incident after immediate action has been performed.

4. Security incidents that require reporting:

    a. Virus, worm, local attacks or other malicious code attacks;

    b. Network or system intrusions;

c. Denial of service attacks;

d. Persistent intrusion attempts from a particular entity;

e. Unauthorized access to ePHI systems and networks containing ePHI;

f. PHI data loss due to disaster, failure or error;

g. Physical intrusion at facility;

h. Theft or loss of portable workstation;

i. Failure or malfunction of security assets (cameras, alarms, etc.); and

j. Any other incident which poses significant risk to company and/or client data.

5. Upon being informed of a security incident the security officer will ensure that actions are taken to mitigate any potential harm.

6. The security officer will conduct a breach investigation.

D. **Breach Investigation:** Prominic.NET will investigate, report, and respond to security incidents that may constitute a breach of unsecured PHI. Any acquisition, access, use or disclosure of PHI is presumed to be a breach unless the security officer demonstrates, through an investigation which includes a risk assessment, that there is a low probability that the PHI has been compromised. Answers to the following questions must be determined as part of the risk assessment:

1. Is the use or disclosure impermissible under the HIPAA Privacy Rule?

2. What is the nature and extent of PHI involved in the breach, including the types of identifiers and the likelihood of re-identification?

3. Was the PHI actually acquired or viewed?

4. Who used the PHI or to whom was the PHI disclosed?

5. To what extent has the risk to PHI been mitigated?

If a determination is made that the security incident resulted in a breach of PHI, notification will be made.

1. All notifications will be made in accordance with the HIPAA privacy rule and Prominic.NET's Breach Notification Policy.

2. All security incidents and their outcomes will be logged and documented by the security officer.

3. All documentation related to the investigation, including the risk assessment, shall be retained for a minimum of six years.

4. The security officer will review and revise the policies on security incident response and reporting as needed and train workforce members on these revisions.

E. **Security Personnel and Implementation:** The security officer has overall responsibility for implementation of this policy.

F. **Workforce Training:** The security officer will train all workforce members on the requirements of this policy.

G. **Modification:** Prominic.NET will review and modify the specifications in this policy as needed to continue the provision of reasonable and appropriate protection of ePHI.

H. **Violations:**

1. Workforce members who violate this policy are subject to disciplinary action, up to and including termination.

2. Anyone with knowledge of a violation or potential violation of this policy must report directly to the security officer.

3. Prominic.NET will not retaliate against any workforce member reporting a violation or potential violation in good faith.