IDS Policy

This policy, and associated procedures for intrusion detection, has been subcontracted to a third-party, Platform as a Service, HIPAA compliant vendor (PaaS Subcontractor). We have verified that their policies and procedures meet or exceed our standards and those of HIPAA and the HITRUST Common Security Framework. As such, we have assurances that strong intrusion detection tools and policies to proactively track and retroactively investigate unauthorized access are used. The PaaS Subcontractor currently utilizes OSSEC to track file system integrity, monitor log data, and detect rootkit access.

Proof of such due diligence is kept by the Security Officer.

Applicable Standards from the HITRUST Common Security Framework

- 09.ab - Monitoring System Use
- 06.e - Prevention of Misuse of Information
- 10.h - Control of Operational Software

Applicable Standards from the HIPAA Security Rule

- 164.312(b) - Audit Controls

Intrusion Detection Policy

The primary means through which Intrusion Detection occurs is through OSSEC. OSSEC is used to monitor and correlate log data from different systems on an ongoing basis. OSSEC generates alerts to analyze and investigate suspicious activity or suspected violations. OSSEC monitors file system integrity and sends real time alerts when suspicious changes are made to the file system.

Additionally, the PaaS Subcontractor uses firewalls monitor all incoming traffic to detect potential denial of service attacks. Suspected attack sources are blocked automatically.

We are responsible for:

- Reviewing generated reports from OSSEC on a monthly basis by the Security Officer.
- Coordinating with the PaaS Vendor to respond to any detected threats.

PaaS Vendor is responsible for:

- Reviewing generated reports from OSSEC on a monthly basis by their Security Officer.
- Actively monitoring the network to detect denial of service attacks.
- Testing all new firewall rules and configurations before being put into production.
- Reviewing all firewall and router rules every quarter.
- Using redundant firewall network perimeters.
- Having all servers use static IP addresses.