TRAFFIK | health

HIPAA Compliance & Security Policy

Internal Procedures

TRAFFIK works directly with our clients in meeting the requirements of the Health Insurance Portability and Accountability Act of 1996 (PL 104-191) and regulations enacted by the Department of Health and Human Services at 45 CFR Parts 160, 162, and 164. (The law and rules are collectively referred to as "HIPAA.")

TRAFFIK reviews the confidential data provided by our client for the purpose of generating, printing, mailing statements, invoices, reports and any other required documents. As a Business Associate of our client we comply with all the requirements listed in the Business Associates Agreement between our client and SO.

TRAFFIK's HIPAA compliance procedure for internal handling of PHI (Protected Health Information) documents is outlined below.

1. **All employees who handle PHI are required to read the HIPAA compliant regulations manual** and sign an agreement form that acknowledges that they have read, are aware, and will be compliant with the requirements set for by the Health Insurance Portability and Accountability Act of 1996 (PL 104-191) and regulations enacted by the Department of Health and Human Services at 45 CFR parts 160-164.

2. **Aggregated data is transmitted by an authorized employee** via our secure FTP site. Each of our clients has exclusive access to their own FTP folder on our FTP site. The exclusive FTP folder is password protected and can only be accessed by authorized employees that have the login and password information. The data contained in these folders cannot be downloaded by anyone other than the Senior Programmers at TRAFFIK. Usernames and passwords are controlled at TRAFFIK by the Director of I.T. and Senior Programmers and by request can be changed at any time. As an additional means of security, passwords are changed on a quarterly basis to ensure a high level of security.

3. **Data is validated and passed through our processing server** by personnel who possess the appropriate passwords to log in to our UNIX data processing network. Access is controlled and limited to authorized personnel.

Backups & Security

Our Data Servers are monitored daily for unusual activity. TRAFFIK has the ability to monitor the activity of password holders who have access to our secure FTP and Data Servers. File transfers are available over sFTP(SSH2). For additional security, we offer RPCrypt, propriety encryption software that encrypts both the data and the mode of transmission.

Our processing servers run on the most stable and secure operating systems available. TRAFFIK hosts in-house Web and Data Processing Servers, allowing for complete control of backup systems, physical and electronic security. Archived client data can be retrieved by request from the client and is provided on basic media (CD/DVD) or via sFTP file transfer from our Data Center.

Managed Network Security

1

MANAGED BACKUP AND MANAGED VAULTING

TRAFFIK's Managed Backup and Vaulting services provide scheduled backup of live business data, restore on demand and vaulting in an offsite location, thus protecting businesses from the loss of essential business data due to catastrophic disaster, human error, software corruption, hardware malfunction or corporate data center environment failure.

2

MANAGED FIREWALL SERVICES

24 x 7 monitoring on dedicated appliances, such as Cisco PIX and Check Point Firewall-1, ensures TRAFFIK's security policies are never compromised.

3

INTELLIGENT MONITORING – SNMP MONITORING

TRAFFIK's Intelligent Monitoring provides SNMP poll/trap and MIB II support for polling and monitoring network devices. TRAFFIK gathers information in real-time SNMP threshold monitoring to provide the operational status of our equipment.

4

HOST-BASED INTRUSION DETECTION (HIDS)

HIDS monitors TRAFFIK's servers and applications for malicious activity and other unauthorized use of host resources. The service includes ongoing monitoring of HIDS agents, security maintenance and alerting on intrusions.

TRAFFIK | health

Thank You