HIPAA and Sarbanes-Oxley Compliance with Sawmill

An Executive White Paper

May 2006

Introduction

In recent years, there have been laws put into place to protect the rights of individuals, require audits on electronic information and hold CEOs and CFOs responsible for the protection of all information within their organizations. The Health Insurance and Portability Act (HIPAA) was enacted by the U.S. Congress in 1996 to protect health care coverage for workers when they change or lose their jobs and also national standards for the electronic transactions, security and privacy of that health care data. HIPAA is meant to improve the health care system by allowing electronic transference of data.

The Sarbanes-Oxley Act of 2002 (SOX) contains many provisions in response to recent corporate malfeasance. The CEOs and CFOs now must certify financial reports and provide independent annual audits to prove that internal controls are maintained for financial reporting. In particular, the Public Company Accounting Oversight Board (PCAOB) has made many requirements of a public company, in the use of internal hardware and software, including information about how transactions are being made, who performs them and who has access to them.

Both Acts have the requirements to:

- Establish internal controls
- Identify controls
- Implement Anti-fraud activities
- Reporting
- Perform annual internal audits
- Update reporting systems

<u>Sawmill can identify and establish internal controls.</u>
The initial setup of Sawmill requires the identification of an Administrator. An authorized Administrator will have access to all information and can run reports on all activity. Each bit of network traffic is tracked and reported on. For security purposes, the Administrator will have the utmost control over the filtering and profiles set in Sawmill. Other users can obtain reports, but not set or delete any profiles, build, modify or update the database of any profile without the authorization of the Administrator. Every file and directory permission can be set for individual or multi-user groups. The permissions values can be set so that some users will only have read access and others will have more permissions to enable them to read, write and execute. In this way, the security of the data can be protected at all times. Permissions can be changed as needed for personnel changes.

<u>Sawmill can identify fraudulent activities.</u>
Sawmill will monitor all incoming and outgoing network traffic. Fraudulent activity can be tracked and reported. Any unauthorized access to your hardware or network will be reported by Sawmill. Every visitor is tracked by their unique IP

address, any unauthorized IP addresses can be reported on, and ultimately blocked.

Sawmill has advanced reporting features to fulfill internal audits.
Sawmill can perform the reporting functions that are needed to have a more controlled and monitored internal network. Consistent internal monitoring and reporting is the key to sustaining a company's compliance with the current laws. The reports can be generated on demand, and analyzed for security breaches, trusted host traffic and to monitor traffic flow.

Sawmill is a cost effective reporting system.
Companies faced with having to add new systems, that provide the detailed reports needed for internal audits can be costly. New hardware and software costs have risen significantly for public companies since these Acts were passed. However with the purchase of Sawmill, companies can in most cases, utilize their existing hardware and see their reports within the web browser of their choice. Sawmill also has the capability of growing with your company. There is no lengthy implementation, training or downtime to installing Sawmill. Sawmill can provide the component of analyzing your internal and external controls that you have put in place to control your customer's health and financial data. Sawmill also fulfills the Control Objectives for Information and Related Technology (COBIT) objective of monitoring and evaluating data. All network activity that could lead to a security breach can be monitored. All of this data can be evaluated to ensure that your internal client's data is secure and has not been compromised.

Summary
SOX and HIPAA have significant impact within an organization. CEOs, CFOs and CIOs are now responsible for signing financial audits based on their internal systems. Those systems are key in establishing the infrastructure for compliance with each requirement of SOX or HIPAA. There are also many other activities within a company that also has an impact on the viability of the company. The strength of Sawmill lies in its ability to perform many functions at one time. It can provide the types of reports needed for compliance, while at the same time provide much needed information about the companies' customers, viability of ad campaigns and even geographical information that will in total add value to any company's business decisions about growth and security.