HIPAA Case Studies

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) provided for the publication of the Privacy Rule which serves as the standard governing organizations subject to HIPAA and its protection of privacy arrangements. The Privacy Rule was first published in 2000. Revisions in 2002 led to the publication of modifications in final form on August 14, 2002.

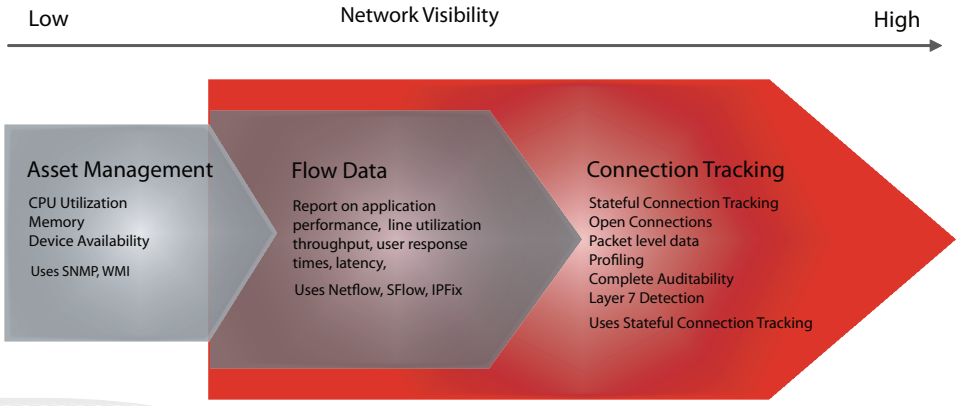
The Privacy Rule applies to health plans, health care clearing houses and to any health care provider who transmits health information in electronic form in connection with transactions that have been designated by the Secretary of Health and Human Services (HHS). The Privacy Rule protects all "individually identifiable health information" held or transmitted by a covered entity.

Consistent application of the Privacy Rule and its objectives is a critical task for all covered organizations. The implementation of PresiNET's TOTAL VIEW ONE system provides a critical element in the management of the organizations' HIPAA obligations by collecting and maintaining a sound record of activities on electronic networks.

TOTAL VIEW ONE

TOTAL VIEW ONE collects data from the business network by focusing on users, applications and the connections they make on a real time basis. The system collects these data by recording every item and storing information in a database that is built from real time log files.

In turn, log files can be archived for recovery at any point in time. The log files are 'signed', making after-the-fact modifications impossible. This ensures that a completely reliable record of network activity can be retained in perpetuity.



This Case Study uses data from two implementations of TOTAL VIEW technology that have critical HIPAA requirements.

The first is a health insurance clearing house that examines claims for health insurance re-imbursement to establish their legitimacy. The second is a very large public agency that delivers services for children and families. Both organizations are fully subject to HIPAA requirements.

HIPAA Case Studies

The Privacy Rule specifies that the Covered Entity should have the ability to track the instances of user and application behaviour on the network. A visibility solution such as TOTAL VIEW ONE can, implemented properly, provide deep insight into the activity of users and applications, supplying the organization with:

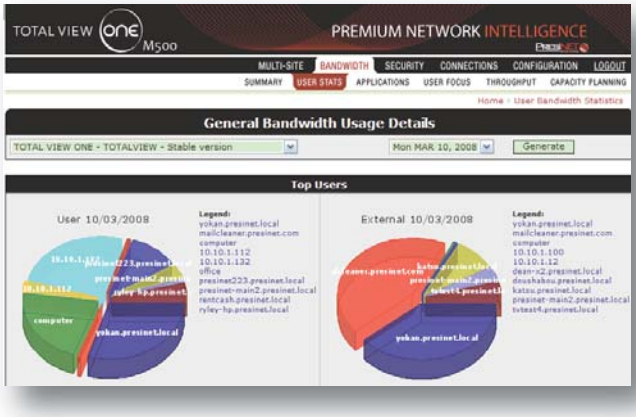
1. Relevant reports to be used by administrators to identify potential policy violations and internal threats
2. Real time information about users and applications traversing the network
3. Long term archival of log data to document policy compliance and individual violations

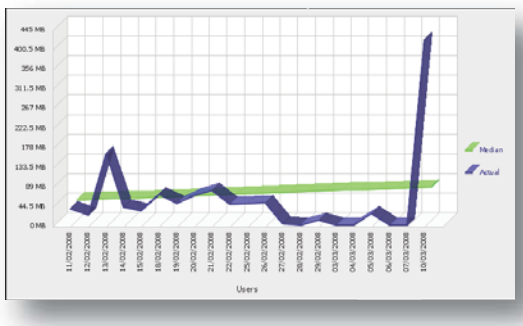
The system should have the ability to generate automatic reports and alerts. The administrator or compliance officer should have the ability to customize these reports and alerts so that they are organizationally relevant.

To be relevant to HIPAA compliance efforts, the visibility should provide real time access into events and current network behaviour, and should enable the access from remote console(s) if required. Using the information, the user can examine the current user and application behaviour to identify current security events on remote, connected networks.

TOTAL VIEW ONE

TOTAL VIEW ONE provides a real time window into the behavior and activities of the users and applications on your network. Information is available in easy to read, drillable format from a secure web portal, enabling effective monitoring of network behavior for behavioral analysis, or network performance troubleshooting.





TOTAL VIEW ONE's unique profiling engine trends user and application behavior on a 28 day rolling window, to easily identify anomalies and potential security violations that go undetected by perimeter security measures not designed to identify them.

A key item to ensuring the visibility system suits itself to assisting the organization with HIPAA compliance is the secure archiving of the source data. TOTAL VIEW ONE:

- Digitally signs the log data
- Encrypts the log files
- Supports long term archival
- Supports easy restoration of archived data

PresiNET Systems Corp
L109 645 Fort St
Victoria, BC
V8W 1G2
www.PresiNET.com
250.405.5380

TOTAL VIEW ONE

Case Study: an insurance claims management company

Highlight Visibility into network activity

Background

One long-standing customer of PresiNET provides health care payers with a total claims management solution that seamlessly and electronically integrates internal claim management systems with external loss control programs. The organization provides a proven, cost-effective system which delivers reductions in claims payments by 3-10% annually.

Pain Point

Because this company processes medical claims, they are privy to a great deal of confidential information. Government regulations like the Health Insurance Portability and Accountability Act (HIPAA) are very strict about what organizations can and cannot do with data, and there would be serious penalties if something were to happen to the data. As their Chief Technical Officer points out, "For us more than others, it's critical to ensure that the environment we operate in is safe and secure." But regulatory concerns were only part of the motivation for approaching PresiNET. "Probably 75% of the reason we went this route is just running a good business."

> "We use the unique connection tracking TVO provides to ensure we have insight into each connection made on our network from inside and outside."
>
> CTO of an insurance claims management company

Implementation

The CTO says the installation was quick. "From the time we signed a contract we had a device installed in just a couple of days. And fairly soon after that we knew we had a good fit. We took some time to go through the system, monitor what it was doing, and look through the data it had generated. We were surprised by the amount of activity we saw."

Outcome

Like many other organizations, this one was previously in the dark about much of their network activity. "We use the unique connection tracking TVO provides to ensure we have insight into each connection made on our network from inside and outside. Previously we simply didn't know. Our executives also enjoy the ability to get reports about what people may or may not be doing online. But probably the biggest benefit for us is that it's a major function of the business that we don't have to deal with. With HIPAA and health care being as important as they are, and security being as important as it is, we would have to hire some senior level staff and buy some very expensive equipment to get the same value and provide the same services."

TOTAL VIEW ONE

Case Study: public service agency

Highlight Secure Archiving

Background

This public agency serves children and families, delivering its services through large numbers of direct employees working on their own, often connected only through electronic means and through significant numbers of agencies that fall into the category of 'associate' under the HIPAA rules. Services delivered include a mix of health and social services requirements.

Pain Point

On an on-going basis, the agency is subject to significant pressure for performance in a public setting that frequently places it under the microscope. Recognizing that services are delivered in large part by employees that connect to systems and data bases remotely, the agency needed to implement a series of measures designed designed to ensure security and the protection of privacy, while maintaining and improving the efficient delivery of services.

> "With TOTAL VIEW ONE, we don't need to wonder about what may be on the network. Now we know."
>
> Network Administrator, public service agency

Implementation

An intensive selection process led to the decision to implement TOTAL VIEW ONE. From the perspective of the managers of IT services for the agency, the ability to "see what is running on the network" is critical. TOTAL . VIEW ONE won the competition, both because the system provides real-time alerts concerning network activity, and the ability to swiftly drill down and identify the sources of anomalies and user and application activites, and because of the secure archiving functionality of the system.

Outcome

The TOTAL VIEW ONE system was successfully implemented in the agency network, and is now a critical element of their network management approach. Administrators have easy access to a wealth of information about the network activities of those accessing its resources, in addition to an independant, auditable log of that access. In addition, the system provides network management tools that have increased network uptime and productivity by helping IT staff to quickly identify the root causes of application slowdowns, and network bottlenecks. "With TOTAL VIEW ONE, we don't need to wonder about what may be on the network. Now we know."