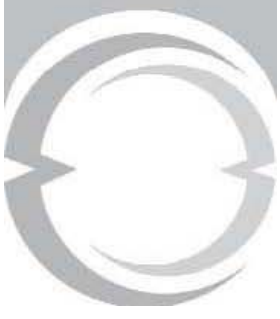
Permeo Technologies

WHITE PAPER

HIPAA Compliancy and Secure Remote Access: *Challenges and Solutions*



Introduction

The Healthcare Insurance Portability and Accountability Act (HIPAA) of 1996 has had an enormous impact on the healthcare industry. Designed to regulate how healthcare-related information is created, stored and distributed, HIPAA affects thousands of hospitals, physicians, insurance providers, healthcare clearinghouses for nonstandard insurance claims, IT professionals, and many other service providers.

HIPAA promises to deliver a number of benefits for both patients and the healthcare industry. At the same time, HIPAA compliancy, especially in terms of security for PHI (Personal Health Information), is an ongoing challenge for healthcare providers and their business partners.

Security is especially challenging for remote access. Distributed user groups, wireless networks, unmanaged devices and a host of viruses expose sensitive PHI to theft, loss and corruption. Endpoint security is critical given the distributed nature of today's Internet-based networks. Healthcare professionals also need to develop security solutions that are both cost-effective and extensible.

Permeo's Base5 product, which delivers on-demand remote connectivity and endpoint security, successfully addresses the demands of HIPAA compliancy for today's healthcare industry.

Competing Demands Under HIPAA Compliancy

Under Title II, Subsection F, "Administrative Simplification," HIPAA outlines a number of specific goals for PHI security.

These goals basically involve four major demands, all of which are critical to compliancy and in close competition with one another. Each demand must be balanced against the others, in terms of technology, resources and financial considerations.

Security

PHI security is at the heart of HIPAA. The "Administrative Simplification" subsection requires organizations to show that they are able to ensure the integrity and confidentiality of PHI, protecting it against theft, loss or unauthorized disclosures. It should also be emphasized that HIPAA compliancy is not a single event but rather an ongoing process. Compliance involves constant monitoring and regular assessments, especially for growing and evolving IT infrastructures. Audit trails for data access must also be generated and archived to provide critical information such as who accessed what, where, how, and when.

Availability, including remote access

Protecting and securely managing information must be balanced against the demand of data access, even from remote locations over the Internet. As more and more healthcare industry professionals use Internet-based communications, the problems of maintaining security continue to grow exponentially.

Cost

Security and data-access requirements must, in turn, be balanced against financial considerations. It has been estimated that the total costs of HIPAA compliance will exceed $17.6 billion over the next 10 years.[1] The total cost of operation (TCO) of the security solution must also be taken into account, from initial implementation and beyond.

Extensibility

A key final consideration involves the remote access architecture. An organization must support communication among a growing number of users beyond the firewall — such as partners, consultants, contractors, and remote employees — without exceeding the budgetary goals of the organization. Ideally, the remote access solution should provide seamless scalability to accommodate the future growth of the enterprise, as well as the development of value chains across the industry.

Secure Remote Access and Endpoint Security Solutions

Traditional Strategies for Secure Remote Access

A variety of strategies and solutions have been developed to address the competing demands of secure remote access under HIPAA.[2] Each solution is based on a Virtual Private Network (VPN)

[1] DHHS Fact Sheet, December 2003.

[2] For additional information about the strengths and weaknesses of VPN architectures, see Permeo Technologies white paper, *The Unified Remote Access Approach: A technical comparison of VPN architectures* at www.permeo.com.

architecture. VPNs are private networks over the Internet with security supported by protocols, encryption such as Secure Sockets Layer (SSL), various security services, and other components.

IPSEc VPNs offer broad application support, with connectivity for almost any IP-based application. On the other hand, IPSec VPNs require thick client software that must be installed and maintained at the user endpoint, whether a PC or laptop. IPSec VPNs also require protocols such as AH, ESP and IKE which are not generally allowed by remote gateway devices such as firewalls.

Another approach is an HTTPS Reverse Proxy VPN. This architecture can support Web applications and simple file shares with existing browsers. However, the architecture does not support non-Web applications without special client "access modes" or "extenders."

In addition, non-Web applications pose a serious problem for HTTPS reverse proxy strategies. Complex — and expensive — provisioning is required, with up to three clients and extensive network administration. Special Web portal interfaces must be used at endpoints, and if special client software is required, support costs can be prohibitive, much like IPSec VPNs.

Endpoint Security: A Critical Part of Remote Access

VPN connectivity features address only half of the challenge involving secure remote access. Endpoint security is equally important, if not more so.

In fact, with today's growing threats from worms, trojans, denial-of-service attacks and other malware, endpoint security can be regarded as the "front line" of network security. Often, attacks on the network are successful because they target unmanaged or poorly maintained endpoint devices, exploiting the vulnerabilities and gaps in endpoint protection.[3]

When evaluating a VPN solution for secure remote access, organizations must consider its endpoint security capabilities with the same diligence as its connectivity capabilities.

Specific areas to examine include the following:

- How well is endpoint security integrated with the VPN? Is deployment of a separate client and management server required?
- How easily can endpoint security be deployed to unmanaged devices? Is thick client software required? Are administrative privileges required?
- How comprehensive is the endpoint security feature set? Key features to look for include cache clearing, cache encryption, malware protection, host integrity checks, and information controls.

To summarize, traditional strategies for secure remote access require a complex and difficult mix of IPSec VPN, HTTPS Reverse Proxy VPNs and endpoint security products. The cost of this complexity is apparent not only in product acquisition and deployment costs, but also in the ongoing operational costs of supporting a number of discrete remote access solutions, each with a unique administrative interface. Each solution contributes incremental client software support, server/gateway administration, and help desk costs.

Therefore, these solutions fall short in meeting the business requirements of today's organizations.

Permeo Base5: Addressing HIPAA Requirements

Permeo is a zero-touch on-demand remote connectivity solution integrating advanced endpoint security and information privacy services.

Permeo's Base5 delivers a unified policy enforcement and management framework that fully integrates SSL VPN, Information Control, Browser Security, Malware Protection, and Host Integrity Checks. Its patent-pending session layer technology uniquely enables a zero touch deployment model in which no remote client administration is required for the delivery of connectivity and endpoint security capabilities.

[3] *Endpoint Compliance Enforcement, An Enterprise Management Associates Technology Study*, January 2005. Available from Permeo at www.permeo.com.

The Base5 solution is made up of two components:

The Base5 Connector is a lightweight program that is downloaded to the endpoint device at the start of each session. The Connector inserts itself at layer 5 of the OSI network protocol stack, intercepting system calls for network resources and redirecting them to Base5, according to corporate policy. It is completely transparent to higher level applications and the underlying operating system. This transparency enables administrators to extend both VPN connectivity and endpoint security to any device, whether managed or unmanaged, without touching the device. The Connector eliminates the need for thick client installation, complex application translation modes, administrator privileges, changes to application and system settings, or reboots.

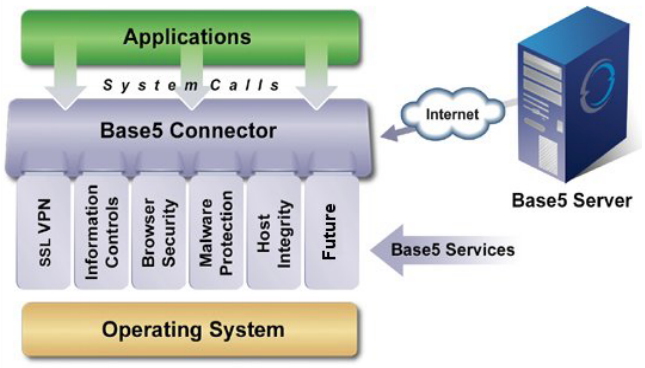
The Base5 Server provides shared gateway and management functions for all Base5 services. Gateway functions include authentication, on-demand software delivery, gateway policy enforcement, and SSL VPN termination. Management functions include policy definition and distribution, monitoring, alerting, and logging. The management capabilities of Base5 are shared across all services–eliminating the need for multiple consoles. The Base5 Server integrates with existing network infrastructure including directories, authentication and audit/logging systems.

The following section examines how Base5 addresses HIPAA compliancy in terms of the four demands previously discussed — security, availability, cost, and extensibility.

Security

Permeo's integrated security and access policies provide advanced remote connectivity and endpoint security.

- **Information Controls** and digital shredding of browser information for data usage compliancy prevent the leakage or theft of confidential application data by controlling what users can do with the data once it arrives on the endpoint. Permeo's Base5 enforces the data usage compliancy policy by allowing the administrator to remove the ability to copy, paste, print, save or print-screen information. At the end of the session, digital shredding removes the remnants of the web applications upon the termination or time out of the secure session. Browser cache, offline content and cookies for the secure session are eliminated from the system, leaving no traceable information.



The Base5 Connector is downloaded "on-demand" to remote devices from the Base5 Server.

- **Host Integrity Checks** prevent unsecured remote device configurations from threatening the corporate network. The Base5 connector validates the posture of the endpoint before connectivity is provided. Based upon the results of the interrogation, connectivity to individual corporate network resources is allowed, limited or prevented, protecting the network from the introduction of malware from unmanaged endpoints. Host integrity checks can be configured to confirm antivirus and firewall protection, as well as operating system and browser version levels, before allowing SSL VPN connections and throughout the session. Additionally, enterprise-specific host integrity checks can be defined. Permeo's Base5 encrypts session information and prevents information eavesdropping by unauthorized users or malware programs such as spyware.

- **Browser Security** protects sensitive information which is stored by the browser during a VPN session, including cache, auto-complete, and offline browsing. For example,

browser cache is encrypted during each connection session and then cleared at the end of the session.

- **Malware Protection** prevents unauthorized remote applications, such as worms, Trojans or latent malware from leveraging the secure connection to attack the corporate network. Each application requesting VPN access is checked against corporate access control rules and is validated via a cryptographic checksum.

Availability

Permeo enables seamless remote connectivity for enterprise applications, providing an in-office user experience for end-users.

- **SSL VPN** service takes advantage of the Base5 Connector to support virtually any enterprise application in their native format via a single user access mode. Users may access applications from a standard portal interface or directly from their desktop, for an IPSec-like "in office" experience.

- **Single Mode Connectivity** enables remote access to any application, including web-enabled and legacy applications, through a simple interface with the look and feel of the user's native desktop.

Cost

Permeo reduces the total cost of ownership for secure remote connectivity. For example, Permeo's customer, Sun Healthcare, reduced their ongoing operational costs by 82%.

- **Simplified Administration** eliminates management of client software, multiple consoles and policy engines. The Base5 unified management console defines and distributes policy, without end user touch, and monitors all connectivity and security features from a simple web-based interface.

- **Zero Touch SSL VPN and Endpoint Security** enables easy and rapid deployment, delivering all Base5 services – SSL VPN, Information Controls, Host Integrity Checks, Browser Security and Malware Protection – without the cost of touching end user devices.

Extensibility

Permeo's Base5 is easily upgradeable to support growth in concurrent users. As a single solution for web applications, portals, client server applications, ftp and legacy applications, Permeo reduces the burden and impact to the client system and management infrastructure.

- **Extensible Architecture** ensures seamless scalability to meet future needs. Base 5 is easily upgradeable to support growth in concurrent users without the constraints of a fixed, obsolete appliance, lowering total operational costs and improving performance by leveraging processor and system technology improvements.

- The ability to manipulate system calls with Base5 can be leveraged beyond the redirection of network requests for VPN purposes. It also makes the Connector an ideal platform for supporting any number of integrated endpoint security services.

Summary

Permeo's Base5 is especially appropriate for supporting the ongoing demands of compliance as well as endpoint security — two aspects critical to HIPAA regulations.

With secure, on-demand remote access capabilities, Base5 allows organizations to provide a spectrum of end users with *controlled*, *auditable* access to both web and non-web applications, while maintaining the essential level of security. Permeo's zero touch approach and integrated management of remote access and endpoint security enable compliance with HIPAA requirements and significantly reduced costs for remote access administration. Plus, by providing extensibility for upgrades and expansion, Base5 ensures that organizations are well-positioned to meet both the evolving needs of the business and the ongoing demands of government-mandated compliance requirements.

By successfully addressing the demands of HIPAA compliancy for remote access, Permeo's Base5 provides a secure, flexible, and cost-effective solution, regardless of the size or growth of the organization. *For more information about Permeo solutions, visit www.permeo.com or call (512) 334-3600.*