HIPAA COMPLIANCE

How NetScreen Meets the Security Requirements of the Health Care Industry

April 2001

A White Paper by
NetScreen Technologies Inc.

Table of Contents

Purpose

The purpose of this white paper is to describe:

- The HIPAA certification process, and
- The NetScreen role in this certification.

NetScreen's goal is to provide a template to the Health Organization that inserts into their HIPAA compliance certification request, showing that the NetScreen portion of their Health Organization security system is HIPAA compliant.

Summary

HIPAA compliance addresses how the Health Organization will implement and coordinate their **business processes** to meet the HIPAA intent described below. HIPAA is a three-part set of rules:

- HIPAA regulations related to e-commerce have already been issued and taken effect to mandate certain technologies, such as Electronic Data Interchange.
- The privacy portion of the HIPAA rules has been more controversial. Much of the established healthcare industry have become vocal critics of the rules, which they say will be too costly and impede patient care.
- A third portion of the HIPAA rules concerns security, and the final version is not yet out.

Management Responsibility

Under the privacy rules, a Health Organization CEO could be held liable for privacy violations and face jail time if successfully prosecuted. This threat may spill over to the technology providers should they mislead the Health Organization in some way.

The HIPAA privacy rules require healthcare organizations to ensure their **business partners** take as much care with patient data as they would. The Health Organization protection process can only work if **ALL** participants of the medical network use secure procedures and know how to apply them correctly.

However, it is highly advisable to assume that any of the adjacent networks can be compromised, so whenever technically possible and economically feasible, it is wise to err on the paranoid side. Health Organizations must take steps to protect themselves from intrusion from the partner network, in case that partner fails to protect their network adequately.

Information System Contribution

As part of their compliance efforts, Health Organizations must institute policies for selection and acquisition of new information systems that require vendors to demonstrate compliance with known HIPAA requirements and a commitment to meet future requirements.

The information systems only help the Health Organization meet some of the line items in the HIPAA compliance statement, **but there are no hard requirements that would specify how equipment would be HIPAA compliant**. The requirements are stated in vague technical terms, leaving it up to the Health Organization management to decide if the equipment meets the needs.

HIPAA provides detailed checklists and reporting material that allows the Health Organization management to **prove** their compliance. Many of the line items pertain to functionalities provided by technology. The administrator must describe how the technology causes them to meet the compliance requirement.

From an information systems perspective, HIPAA has two important characteristics:

- HIPAA is completely scalable, therefore it covers all facilities ranging from the smallest one-person organization to the largest institutions.
- HIPAA is technology neutral. For example, all organizations will be required to install audit-control mechanisms to record and examine system activity. However, the organizations are left to decide on which methods and technologies to use to do this.

A New Perspective on Security

With the introduction of the Internet, sharing patient information over a far-flung regional network that links multiple hospitals, clinics, and doctors' offices has become all the more complex.

Initially, HIPAA expectations were that any electronic data moving within the confines of the Health Organizations' dedicated network did not have to be encrypted, and all data transferred over the Internet had to be encrypted.

So most organizations felt that not being on the Internet was a sufficient safeguard. Unfortunately, access to the Internet has become indispensable for most Health Organizations, so they must consider that their network is exposed to the Internet in one or more locations, and therefore measures must be taken to **protect the network from Internet based attacks**.

The activity level in Medical Facilities is so high, and so many people are sharing the network, that all health facilities must **protect against data theft from the inside**. Industry experts estimate that 65% to 75% of data thefts will likely originate from within the Health Organization.

The number of Health Organizations that need to exchange data is growing exponentially as data becomes electronic and therefore easier to exchange. Deploying a private network between facilities becomes expensive, difficult to manage and difficult to charge back to the growing number of independent participants. The Internet is the only ubiquitous network that economically reaches all the Health Organizations.

Security Inside

Most security administrators have viewed security as an edge device that protects against Internet intrusions and encrypts data that will travel over the Internet. Although

HIPAA does not immediately require it, it is only a question of time before authentication and encryption are required on private links and for data to be encrypted inside the trusted networks.

After all, the responsibility conveyed by HIPAA is to implement a security process that permeates all portions of the Health Organization, protecting data as it is accessed and as it travels **anywhere** throughout the participating organizations.

HIPAA Certification Process

Public Law 104-191, The **H**ealth **I**nsurance **P**ortability and **A**ccountability **A**ct (the **HIPAA** Act), was signed into law on August 21, 1996. For more information, you can visit www.hcfa.gov/hipaa/hipaahm.htm. Having its roots in the 1993 Clinton healthcare reform proposals, the intent of this law is to:

- Improve the efficiency and effectiveness of the healthcare system by standardizing the interchange of electronic data for specified administrative and financial transactions; and
- Protect the security and confidentiality of electronic health information.

Unless these dates are changed in the near future as a result of ongoing debates in the Bush administration, large Health Organizations have until August 17, 2002 to comply with the HIPAA regulations and small Health Organizations have until August 17, 2003 to comply. Some of the compliance items are being rolled out in stages with the Privacy portion scheduled to be in place by April 14, 2001.

The DHHS (Department of Health and Human Services) manages the application of this law. It spells out "what" has to be protected but remains intentionally generic on "how."

The law provides for significant financial penalties for violations:

General Penalty for Failure to Comply:

- Each violation: $100.
- Maximum penalty for all violations of an identical requirement: May not exceed $25,000.

Wrongful Disclosure of Individually Identifiable Health Information:

- Wrongful disclosure offense: $50,000, imprisonment of not more than one year, or both.
- Offense under false pretenses: $100,000, imprisonment of not more than 5 years, or both.
- Offense with intent to sell information: $250,000, imprisonment of not more than 10 years, or both.

HIPAA Compliance Stamp

The Health Care Manager cannot delay this implementation since other organizations are now making HIPAA compliance mandatory. State and federal legislation, professional and standards organizations, and internal organizational risk management departments are also driving the need for security measures. Many states, for example,

regulate the use of electronic signatures and medical records. The **J**oint **C**ommission on **A**ccreditation of **H**ealth care **O**rganizations (JCAHO) also addresses security and confidentiality issues, and require a firm commitment to reach HIPAA compliance in time to qualify for accreditation.

The Health Care Manager must address the balance between sharing data and protecting its confidentiality. This requires a process where they:

- Define levels of security and confidentiality for different categories of information
- Define storage and access rules in respect of these categories
- Define user profiles based on their access rights to categories of information
- Provide easy to use tools to all users to operate within the process regulations
- Define rules for the release or removal of the medical record
- Define how information is protected against unauthorized intrusion, corruption, or damage
- Define and practice the reaction protocols when confidentiality and security are violated

Remembering that a business process involves people, the Health Care Manager must also:

- Make all end users realize their responsibility in keeping information confidential
- Verify that users are respecting the process regulations

HIPAA will affect all health care organizations at least as much as the Year 2000 problem. In particular, organizations should focus on HIPAA compliance in the following areas:

- ***Electronic Data Interchange (EDI)*** such as transactions for health plan enrollment, eligibility, claims payment, premium payment, coordination of benefits, and referral/authorization. Fundamental requirements include integrity control (to ensure the validity of transmitted information) and message authentication (to ensure that the message received matches the message sent). Health care entities must also employ either access controls or encryption, except that if information is transmitted across an "open" network such as the Internet, then encryption becomes mandatory. Other requirements include alarms, audit trails, entity authentication, and event reporting.
- ***Storage and reporting of identifiers*** such as Patient IDs, provider IDs, payer IDs, and employer IDs will be standardized under HIPAA for purposes of electronic transactions. As a result, information systems devoted to administrative, financial, and clinical applications must be able to capture, store, and report these identifiers.
- ***Protecting confidentiality*** of individually identifiable patient information in an automated system

HIPAA Technology

Cutting-edge technology do not make networks secure; they are only enablers. The key is to ***make security and confidentiality part of the Health Organization business process***. As a corporate issue, security and confidentiality cut across diverse areas of

technology, organization, and regulation. The IT managers can shoulder the responsibility for putting bullet-proof systems in place, but the ultimate responsibility remains in the hands of the operational managers who own the data and who have authority over the end-users. The security systems must enable the operational manager to easily understand the infractions and manage end-users who do not comply. Assuming that the IT staff has implemented their systems properly, the Operational Manager becomes accountable for the HIPAA penalties, and is therefore motivated to carefully monitor this process.

HIPAA compliance guidelines specify certain rules that the Health Care process must meet to remain within the law. Organizations and vendors in the health care industry should understand the elements of HIPAA and be aware of the required changes. Providers and health plans need to review their current information systems for HIPAA compliance. But that's just the beginning. Organizations should also closely review their current confidentiality and security practices--and most likely enhance them.

To eliminate this risk, the Health Care Manager needs to document the organizational policies and protection processes.

- *Administrative procedures*---documented general practices for establishing and enforcing security policies
- *Physical safeguards*---documented processes for protecting physical computer systems, buildings, and so on
- *Technical security services*---processes that protect, control, and monitor access
- *Technical security mechanisms*---mechanisms for protecting information and restricting access to data transmitted over a network

One important portion of this documentation is the verification that all equipment used in their security process meets the minimum requirements required in the HIPAA regulations.

NetScreen Role in HIPAA Compliance

This section deals with requirements stated in the HIPAA document “Security and Electronic Signature Standards, Section 4. Technical Security Mechanisms to Guard Against Unauthorized Access to Data that is Transmitted over a Communications Network, ” published in 1998 and revised latest in 1999.

Firewalls

The Firewall capabilities of NetScreen devices is the basic building block permitting to keep all networks secure by:

- **Packet Filter:** The most basic firewall function, it filters connection requests based on source and destination addresses and ports;
- **Proxy server**: Inserts advanced analysis of certain protocol types such as SMTP and FTP between the source and destination to protect against brute force attacks and sophisticated attacks that may exploit protocol weaknesses.

- **Stateful inspection:** Goes beyond Packet Filter and Proxy by tracking the on-going evolution of each connection individually and of all connections as a whole, to ensure that they meet expected behavior patterns.
- **Network Address Translation:** NAT conceals client addresses in an internal network under a single address;
- **Transparent Mode:** despite the hiding function provided by NAT, specific devices can be addressed directly using a public address, allowing for example, a VPN tunnel to be established between a computer inside one network, with a server inside another network. This is also useful when installing firewalls inside the network to protect specific servers.

Authentication

If digital signature is employed, the following three features must be implemented:

- Message integrity,
- Non-repudiation,
- User authentication.

Other implementation features are optional.

Software verifies the identity of a user who logs onto a network or the integrity of a transmitted message. Authentication solutions include user registration policies that identify and track users without having to make changes at the user desktop. Security managers can centrally control access to the network.

In “Security and Electronic Signature Standards, Section 10”, HCFA states that:

- “HIPAA directs the Secretary of the Department of Health and Human Services to coordinate with the Secretary of the Department of Commerce in adopting standards for the electronic transmission and authentication of signatures with respect to the transactions referred to in the law. This rule was developed in coordination with the Department of Commerce's National Institute of Standards and Technology. We propose to adopt a cryptographically based digital signature as the standard.” “Whenever a HIPAA specified transaction requires the use of an electronic signature, the standard must be used. It should be noted that an electronic signature is not required for any of the currently proposed standard transactions.” *NetScreen is a key participant in the use of digital signatures for user authentication to provide access into a network and for the use of digital signatures to establish VPN tunnels.*
- “In the electronic environment, the same legal weight associated with an original signature on a paper document may be needed for electronic data. Use of an electronic signature refers to the act of attaching a signature by electronic means. The electronic signature process involves authentication of the signer’s identity, a signature process according to system design and software instructions, binding of the signature to the document and non-alterability after the signature has been affixed to the document. The generation of electronic signatures requires the successful identification and authentication of the signer at the time of the signature.” *NetScreen recommends the use of digital signature for authenticated access to the network to assure a non-refutable time stamp of*

each access, assuring the ability to prevent illegal access and prosecute those who abuse their rights.

- "The proposed standard for electronic signature is presented at § 142.310 and would be digital." *The acceptance of this standard is imminent.*

NetScreen Digital Certificate Authentication

Based on the statements above, all users will soon have to use some type of digital authentication technology. That will most likely be X.509 certificate technology. All NetScreen devices can use these certificates for 1) user authentication as well as 2) VPN tunnel authentication.

All X.509 certificate manufacturers are supported, therefore the Health Organization can outsource the certificate management or manage their own. Users needing to pass through a NetScreen device located either in front of a server or as a network edge device will be able to transparently pass (without an ID and password) through the device since all their connection requests will be signed using their certificate.

Protection from Threats Caused by Employees

Many threats result from activities initiated by user workstations inside the protected network, such as accessing Internet sites that do not pertain to the Health Organization business, exposing the entire network to remote control from these sites through downloading of Trojan Horses and such spy tools.

URL blocking: One of the basic firewall functions is to call a URL list server to verify that the Web site for this URL is within acceptable category. In addition to protecting from Trojan Horses, they also prevent employees from wasting their time surfing for personal reasons.

Encryption Requirement

HCFA states that:

- "Each organization that uses communications or networks would be required to protect communications containing health information that are transmitted electronically over open networks so that they cannot be easily intercepted and interpreted by parties other than the intended recipient, and to protect their information systems from intruders trying to access systems through external communication points. When using **open networks** (like Internet), some form of encryption should be employed. The utilization of less open systems/networks (that we will call Semi-Trusted Networks) such as those provided by a value-added network (VAN) or private-wire arrangement provides sufficient access controls to allow encryption to be an **optional feature**."

One can conclude for now that the HIPAA requirement is to ONLY encrypt data transported over the Internet. However, the FBI and all security professionals keep warning us that 65% to 75% of data theft will occur inside the Trusted Network. If at all possible, it would be wise to implement a solution that may go further.

Data can be encrypted at different levels:

- Creating a VPN tunnel between the edge devices protecting each network – as requested by HIPAA;
- Between a workstation (wherever it may be) and the firewall protecting the Trusted Network – using a VPN Client on the workstation.
- Between a workstation (wherever it may be) and a firewall controlling a subnet containing only trusted servers.

The third option has been desired for a long time, and has been attempted by using DMZs, however they were not acceptable due to lack of encryption power of legacy firewalls. NetScreen devices have broken this logjam by providing line speed encryption at a very low cost as compared to legacy firewalls.

Encrypting the Semi-Trusted Networks

The directives state that connections between Semi-Trusted Networks do not need to be encrypted. However, they should receive the same level of control and scrutiny as the Internet interface. A WAN link between two Health Organizations should not allow **just anyone** from one organization to access any system in the other organization. We must step back and recognize the true meaning of the HIPAA directive: to protect the data entrusted to the Health Organization.

A NetScreen device installed at that Semi-Trusted interface is cheap insurance, providing user Authentication at the NetScreen interface to control what outsiders have access to what devices inside the Health Organization's network. As PKI certificate use becomes prevalent, they can be used for authentication where the connection request is automatically signed using the user's certificate.

Encrypt all the Data, all the Time

VPN tunnels should not be limited to linking Open-Networks and Semi-Trusted Networks. All data transmitted from anywhere to anywhere (even inside the protected network) should really be encrypted, based on the industry-accepted fact that 65% to 75% of data thefts are executed from inside the protected network. This has not been feasible before NetScreen because this amount of encryption would require too much CPU power from the servers and no device had the horsepower to deal with this much encryption economically.

This can now be accomplished very simply by installing a basic NetScreen-5 in front of each server. A NetScreen-5:

- Provides about 8.8 Mbps of full duplex 3DES encryption with very little latency,
- Serves as a security device to protect this server from brute force intrusions emanating from the protected network, and
- Manages data flow using its Traffic Shaping feature.

Several servers can be located in a LAN segment behind a single NetScreen device. A NetScreen-100 can be used to handle volumes up to nearly 100 Mbps full duplex.

User Level Encryption on all Workstations

The users end of the VPN tunnel can be terminated at the user workstation using a variety of IKE IPSec compatible client software from NetScreen or other vendors, including the Microsoft Windows 2000 IPSec client or legacy software such as Check Point's SecuRemote.

Encrypting all the data will also eliminate the daunting task of identifying the types of information that must be encrypted since all data will be encrypted. It would be easier to encrypt all data, regardless of their routing.

Encryption Types Required

Encryption converts data for transmission over any network using an algorithm that allows only the intended receiver to decode it at the other end. NetScreen support the two main cryptographic methods are **secret key** and **public key**. In secret key, both sender and receiver use the same "secret" key to encrypt and decrypt. Public key encryption involves both a private and a public key. The sender can use the receiver's publicly available public key to encrypt a message; the receiver uses their private key to decrypt it. The secret key method requires sending the key over unsecured lines to the recipient. Since the owner never sends their private key, the Public Key method is preferred for the long term since the users are more accountable.

Encryption Level

HCFA states "A level of encryption protection equivalent to that provided by an algorithm such as Triple 56 bit DES (3DES) defined as 112 bit equivalent for symmetric encryption, 1024 bit algorithms for asymmetric systems, and 160 bits for the emerging Elliptical Curve systems" is recognized by HCFA as minimally acceptable. HCFA reserves the right to increase these minimum levels when deemed necessary by advances in techniques and capabilities associated with the processes used by attackers to break encryption (for example, a brute-force exhaustive search).

NetScreen supports 3DES encryption using MD5 and SHA1 authentication, which should allow it to interact with the great majority of other encryption devices involved in a HIPAA network.

Encryption Device

- HCFA states "**Hardware encryption** methods are acceptable. These solutions allow ramping up to very large traffic volumes using symmetric "private" key devices that handle speeds in the Gigabit range and beyond". *This precisely targets NetScreen devices.*
- HCFA states: "**Software Encryption** methods are also acceptable. The encryption can be implemented at several levels of the process, such as:"
  - **"VPN in-stream encryption** implementations in the transport layer, based on Secret Key or Public Key methods." *This is NetScreen's strongest capability. However, the location of the encryption process is one of the crucial security aspects described in more detail below.*

- **“Secure Sockets Layer (SSL)** based on standard commercial implementations of PKI.” *NetScreen is not affected by SSL sessions that are being decrypted by Web applications inside the protected network. NetScreen does not provide SSL termination or acceleration.*

NetScreen Web UI uses SSL encryption for device management. It uses the equivalent SSH for CLI access. The Health Organization Manager should never accesses the device in clear text mode.

“Offline encryption/decryption of files at the user sites before entering the data communications process. These encrypted files would then be attached to or enveloped within an unencrypted message. Once again, appropriate Secret key or Public Key methods are acceptable.” This method will be used mainly to deliver documents to entities outside the trusted community (i.e. with whom the Health Organization Manager has not established a VPN relationship). *NetScreen does not offer any service in this area.*

Intrusion Detection

Intrusion detection systems trigger alerts when unauthorized users enter the network, and automatically removes them when they finish their connection. Accepted methods are:

- Formal Certificate Authority-based use of digital certificates. *NetScreen supports all public CA hierarchies that use X.509 technology.*
- Locally managed digital certificates, providing all parties to the communication are covered by the certificates. *NetScreen supports all public CA hierarchies that use X.509 technology.*
- Self-authentication, as in internal control of symmetric "private" keys. *NetScreen supports Shared Secret private key generation using IKE*.
- Tokens or "smart cards" used for authentication. Tokens involve overall network control of the token database for all parties. *NetScreen supports SecurID and is open to add new technologies as needed.*
- Out-of-band Authentication processes are also acceptable. *Health Organization Manager could use third-party software that commands the NetScreen device to add a new user authentication and subsequently removes it.*

Other authentication methods mentioned in the HIPAA document do not apply directly to the NetScreen environment, however the Health Organization Manager could develop solutions that interface with the NetScreen devices to allow users to be accepted automatically following authentication using one of the following methods:

- Telephonic identification of users and/or password exchange.
- Exchange of passwords and identities by U.S. Certified Mail.
- Exchange of passwords and identities by bonded messenger.
- Direct personal contact exchange of passwords and identities between users.

Single Login Capability

HIPAA recommendations state:

- "A system cannot allow, for example, several providers to use the same device simply by using the same password and logon for the sake of convenience. But on the other hand, users cannot be expected to go through lengthy logins and logouts to share a device."

Using certificates, users will be able to transparently sign their connection requests, thus eliminating the need to login to the NetScreen security interface.

Reporting and Tracking

NetScreen reporting is complete and allows subsequent detailed reporting capabilities to detect inappropriate behavior that may not have been detected in real time, and sufficient tracking information to identify the perpetrator and allow prosecution. NetScreen alert tracking and SNMP interfaces allow immediate response to intrusions.

Conclusion

Virtually every health care system in the country is trying to come to terms with numerous complex security issues. What they are finding is that security policies must be pervasive---security must be end to end. A well-balanced strategy that integrates organizational policy, regulatory compliance, and top-notch network technology into the culture of an organization can achieve this goal. The end result will prove that the electronic process of securing information will ultimately be an improvement over the paper system that allows virtually anyone to pull a patient's paper medical record off a carousel.

NetScreen Technologies line of integrated security systems and appliances include custom-developed technologies that are ideal for the health care industry. NetScreen has designed the GigaScreen ASIC to relieve the performance bottleneck that has generally been associated with software-based security products running on servers as well as hardware-based security products that rely on third-party chip technologies. Each single GigaScreen ASIC provides hardware firewall, IPSec virtual private network (VPN), authentication, public key infrastructure (PKI), and network address translation (NAT). Hardware firewall functions include TCP header parsing, session lookup and policy lookup. In terms of VPN features, the GigaScreen ASIC offers 1.2 Gigabit per second DES, 400 Mbps Triple DES as well as accelerated MD-5 and SHA-1 features. PKI and NAT acceleration also are included in the GigaScreen. In a system level design, a GigaScreen ASIC is connected to a RISC processor through a multi-bus architecture to accelerate CPU-intensive security functions. This multi-bus architecture uses both the PCI-bus and a direct connection into the system memory that is used for packet and session data. In contrast with competing silicon and system designs that use the PCI bus for all communication, this increases performance by easing the burden on the memory bus and freeing the central processing unit for other tasks.

Along with ASIC technology, NetScreen products implement a custom-developed operating system that improves performance and prevents hackers from cracking the

underlying operating environment. Called ScreenOS, this underlying operating system software that provides the features needed to implement network security and the associated policies for any NetScreen security appliance or system. When establishing or managing any firewall, VPN encryption or traffic shaping functions, ScreenOS offers the configuration, management and monitoring tools required. Rather than being based on "open source" operating systems that can be cracked, ScreenOS is a proprietary operating system developed by NetScreen.

NetScreen's line of security systems and appliances stands alone in meeting the new generation of security requirements. The company's second-generation, hardware-based security solutions are meeting the market's new security requirements. NetScreen's solutions combine stringent security capabilities while at the same time maintaining fast performance. They also are easy to deploy and manage allowing them to effectively be turned on and left alone. And NetScreen's product line meets the needs of the largest and fastest access networks all the way down to the requirements of a single end user.

Additional References

NetScreen also recommends that organizations use the Confidentiality and Security Checklist for HIPAA available at http://aspe.os.dhhs.gov/admnsimp/nprm/seclist.htm.

Other resources:

- *American Health Information Management Association (AHIMA)*---benchmark information, case studies and interim steps for getting started---http://www.ahima.org/
- *Computer-based Patient Record Institute (CPRI)*---good tools for developing confidentiality policies---http://www.cpri.org/
- *Department of Health and Human Services HIPAA*/administrative simplification Web site---Latest news on regulations and current proposed rules---http://aspe.os.dhhs.gov/admnsimp
- *"For the Record: Protecting Electronic Health Information"*---National Academy Press, 1997): 800-624-6242(full report--- http://www.nap.edu/
- *HIPAA Transaction Implementation Guides from the Washington Publishing Company*---http://www.wpc-edi.com
- *Links to other HIPAA sites*---http://www.hcfa.gov/medicare/edi/hipaaedi.htm
- *Subscribe to e-mail release of HIPAA documents, such as "Notice of Proposed Rulemaking"*---http://www.hcfa.gov/medicare/edi/admnlist.htm

For more information on security and health care:

- Computer Security Institute--- http://www.gocsi.com
- HIPAA Proposed Security Rules--- http://aspe.os.dhhs.gov/admnsimp/index.htm
- Information Systems Security Association, Inc.--- http://www.issa-intl.org
- International Computer Security Association--- http://www.icsa.net
- International Information Systems Security Certification Consortium---http://www.isc2.org

