

Security Solutions for Healthcare

Implementing security solutions in response
to proposed HIPAA requirements.

Requirement for Secure Healthcare Data

Like many other industries, electronic data acquisition, storage and access have the potential to streamline healthcare delivery and greatly reduce costs associated with paper transactions.

This is particularly true in today's world of geographically distributed healthcare organizations, including Integrated Delivery Networks (IDNs), where the benefits of using high-performance, multimedia networks to exchange healthcare information are significantly magnified.

In order to allow access to healthcare information electronically at all points where it is required, the need to appropriately secure data becomes a significant concern. Healthcare stakeholders, including patients, caregivers and administrators, must be confident that any sensitive medical information exchanged over networks will not be compromised, and will be viewed only by authorized individuals.

In order to formally address these healthcare information security concerns, legislation was included in the US Health Insurance Portability and Accountability Act (HIPAA-also known as the Kennedy Kassebaum Bill), passed on August, 1996. HIPAA includes a section entitled Administrative Simplification, which includes requirements for security of patient-identifiable healthcare information. In August 1998, HCFA and the Department of Health and Human Services released a Notice of Proposed Rule concerning security and electronic signature . This Proposed Rule suggests standards for the security of individual health information and electronic signature for use by health plans, healthcare clearinghouses and healthcare providers. These healthcare stakeholders would be required to use the security standards to develop and maintain the security of all electronic health information.

A Structured Approach to Security

The security threats faced by any healthcare organization are constantly evolving. The number of ways in which these threats manifest themselves are as numerous as the people, locations and technologies that are found inside an organization. In order to counter such security threats, as well as meet any requirements laid down by HIPAA, it is necessary for a healthcare organization to review its security requirements, and define a security policy, which addresses security threats from administrative, physical and technology perspectives.

Existing healthcare security policies are often implemented at different levels throughout the organization. Security technology varies amongst different departments and user groups within a healthcare organization. Some departments have employed security technology for electronic data in varying degrees, while others have not. This makes it extremely difficult to achieve a common security environment that will address the real threats to an organization and comply with proposed HIPAA regulations.

Nortel Networks* recommends a structured approach to network security. By creating a formalized ongoing security initiative, which includes a number of steps, healthcare organizations will be able to benefit from the efficiency of electronic data access, while meeting proposed HIPAA requirements. These steps include:

- Appointing individual(s) responsible for defining and executing a security policy
- Carrying out a review of existing security capabilities
- Identifying security deficiencies that must be addressed to meet desired security level (including proposed HIPAA requirements)

- Defining security plan and identify resources required
- Implementing the security plan
- Carrying out regular security audits

In order to carry out each of these steps effectively, expertise in the areas of process engineering, corporate security and network security is required. Although it is possible that a single healthcare organization may have all of this expertise on staff, where this is not the case, it is recommended that a healthcare organization work with third-party security experts to define and execute a security strategy that is effective and complies with HIPAA. This is particularly true for the analysis and implementation of secure network systems.

If properly deployed, network security can allow healthcare organizations to safely share information amongst healthcare stakeholders, while guaranteeing scalability and extensibility of the security system. As a healthcare organization's network expands to permit physicians and patients to have secure data access, the requirement for a secure network architecture that can be easily expanded becomes obvious. Flexibility in secure network infrastructure can permit simple adoption of new technologies such as secure virtual-private network (VPN) services, which can significantly reduce network costs when compared to traditional leased-line deployments.

Nortel Networks, together with our partners, offer extensive experience in enterprise networking and network security, and can provide the expertise required for a healthcare organization to define a network security strategy, in-keeping with HIPAA.

¹ This document can be found at the following web page:
http://erm.aspe.hhs.gov/ora_web/plsql/erm_rule?user_id=&rule_id=62

HIPAA Security Requirements

The Security and Electronic Signature Standards of the HIPAA legislation include core recommendations regarding the security of an individual's health information. Note that these HIPAA requirements apply to all organizations handling patient-identifiable health care information, regardless of their size. The major procedure requirements which have been implemented to guard data integrity, confidentiality, and availability as well as to guard data against unauthorized access to data transmitted over a communications network can be grouped as follows:

1. Administrative Procedures
2. Physical Safeguards
3. Technical Security Services and Mechanisms

The specific organizational practices related to security include:

- Security and confidentiality policies
- Appointment of information security officer(s)
- Education and training programs
- Sanctions for security breaches

As part of the information technology requirements (points 2, 3 & 4 above), require that technical policies and procedures are defined specifically for the following eight areas:

- User authentication
- Access controls
- Audit trails
- Physical security & disaster recovery
- Protection of remote access points
- Protection of external electronic communications
- Software discipline
- System Assessment

HIPAA regulations do not stipulate, however, specific technologies to address these areas, allowing maximum flexibility as network security products and technologies advance. Nortel Networks Security Solutions, when deployed in the framework of a structured security plan, can enable a healthcare organization's network to meet the requirements of the proposed regulations.

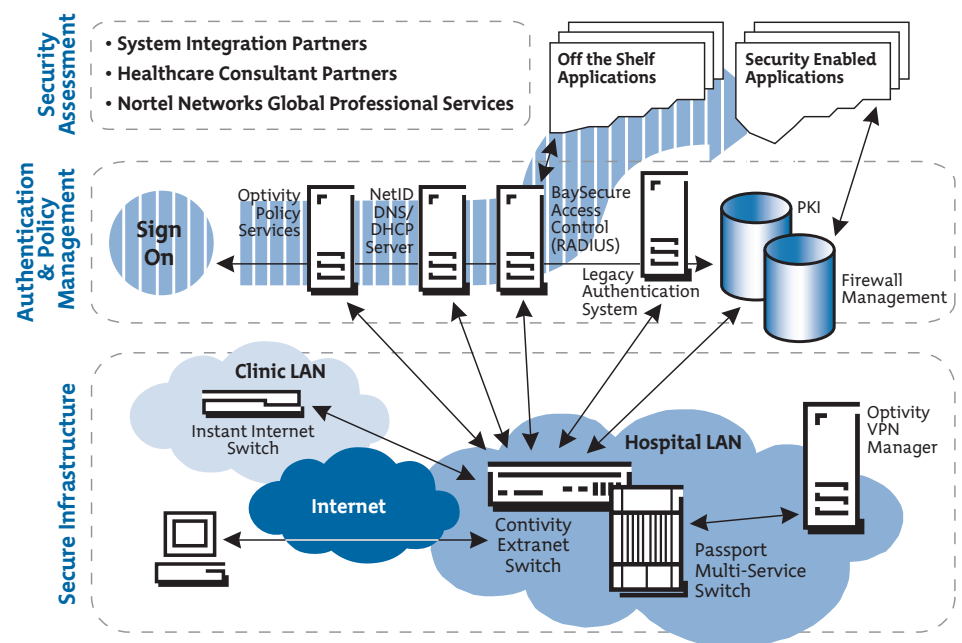
Nortel Networks Solutions for Healthcare Security

Nortel Networks has developed a portfolio of security solutions and expertise upon which healthcare organizations can develop the foundation for a secure network. This portfolio can be divided into three categories: Security Assessment, Authentication and Security Policy Management, and Secure Infrastructure.

The architecture of the Nortel Networks Security Solutions Portfolio is shown in Figure 1. Nortel Networks security solutions offers a broad choice of solutions services, along with a portfolio of security-enabled products that can inter-work with other standards-based equipment, maximizing existing investment. The nature and security status of a healthcare organization, as well as its existing infrastructure, will determine whether some or all components of Nortel Networks' security solutions would be applicable.

Nortel Networks has the resources and expertise to play an important role in any healthcare organization's security assessment. In collaboration with our security solution partners, Nortel Networks can work with a healthcare organization to assess its current security status, and define a network security strategy which meets the organizations security policy, defined in the context of proposed regulations.

Figure 1: Nortel Networks Security Solutions Architecture.



The security assessment could include review of security-enabled applications (those employing password or token access, for example), in addition to the underlying authentication, policy management and secure network infrastructure. With our understanding and expertise in high-availability, reliable networking, Nortel Networks is also positioned to work with healthcare organizations to plan physical network security and disaster recovery policies and procedures. Such steps will help to make patient data secure and available, should catastrophic events occur which have the potential to impact network or data access.

Nortel Networks security solution includes security policy management and authentication for networks supporting the transmission of patient-identifiable information. Products including Optivity* Policy Manager and BaySecure* Access Control RADIUS Server, define and control the network resources, application and data that healthcare staff can access remotely, or transmit between hospitals or clinics. These components interact with the underlying secure network infrastructure, where the user access control is actually enforced.

The secure infrastructure layer provides the physical access to the secure network for healthcare employees internally, via remote clients and between VPN-connected facilities, based on user authentication and defined security policies. This secure infrastructure also carries out the tunneling and encryption (up to Triple-DES), packet filtering and routing required to guarantee privacy of patient data as it traverses VPNs employing “public” network links, including the Internet.

Security Assessment

Nortel Networks, along with healthcare partner organizations, provides extensive experience in the operational requirements of security, both at the network and the application level.

Our healthcare security partners include respected consultants and system integrators who provide extensive healthcare security knowledge and experience. These partners can carry out security assessment, and provide security recommendations and strategies related to security policies, physical security, disaster recover and network security, in collaboration with healthcare customers and Nortel Networks. Nortel Networks Global Professional Services Organization provides network-consulting capabilities at a number of different levels, which can be applied to the planning and deployment of a secure network:

- **Implementation Services:** Basic, Intermediate and Advanced Start-Up Services that meet our customers’ initial network set-up and implementation needs
- **Assurance Services:** Ongoing network support that fits customers’ next-business-day, same-business-day, or around-the-clock network needs
- **Premium Services:** Platinum, Gold and Silver packaged services that supply customers with access to the highest-levels of technical support and value-added service
- **Performance Services:** Strategic network planning services that enhance network operations and maximize network performance

Depending on the level and type of expertise a healthcare organization requires to execute and support their security plan, an appropriate level of service and support from Nortel Networks and its healthcare security partner organization can be provided.

Authentication & Policy Management

The following components enable user authentication and security policy management over the secure network infrastructure. These products interact with the secure infrastructure to provide higher-level security capabilities.

Optivity Policy Services

Optivity Policy Services (OPS) is a sophisticated suite of policy management software that enables end-to-end Quality of Service (QoS) and security management for data networks. It offers a proactive management framework that allows network managers to automatically enforce business-level policies — such as QoS levels and access privileges — on behalf of users, groups, and applications. Optivity Policy Services enforces policies that control the treatment applied to traffic by Infrastructure Layer devices by using an open, standards-based approach.

Data traffic on a network is normally handled on a best-effort basis. That means that critical healthcare applications such as patient record access are given the same priority as email and non-critical Web traffic. Optivity Policy Services solves this problem by giving network managers a means to enforce business policies that prioritize critical applications to ensure they receive preferential treatment from the network.

Optivity Policy Services employs standards-based interoperability and policy control, including support for the Common Open Policy Services (COPS), Differentiated Services (DiffServ), and Lightweight Directory Access Protocols (LDAP V3). In addition, Optivity Policy Services supports all major directory systems — Netscape Directory Server, Novell eDirectory, and Microsoft Active Directory.

BaySecure Products

To protect sensitive data from unauthorized access, BayRS*/BaySecure products provide a broad array of solid security features. BaySecure software provides automatic detection and lockout of unauthorized individuals, and controls access by application, department, or user in any combination to provide additional security. The BaySecure line of products includes BaySecure Access Control RADIUS Server.

BaySecure Access Control RADIUS Server (BSAC) controls user access to network-based applications and services based on policies and identification information stored in a standard directory (for instance LDAP). BSAC defines a certified and encrypted channel between the user and application or service. User A can have access to sensitive patient data applications, whereas User B can have access to only hospital maintenance records.

NetID IP Services Management Software

NetID* is a solution from Nortel Networks for powerful, scalable, fault-tolerant, Internet Protocol (IP) addressing, and Domain Name Service (DNS) and Dynamic Host Configuration Protocol (DHCP) management. NetID automates and integrates IP addressing, as well as DNS and DHCP management.

NetID supports DHCP Client Pools, bringing security to DHCP by restricting dynamic address assignment to clients with known MAC addresses or client identifiers.

Public Key Infrastructure (PKI)

Nortel Networks security solutions are designed to operate with public key infrastructure (PKI) solutions from most popular PKI vendors including Entrust and Verisign.

PKI provides a comprehensive standards-based solution that offers enterprises a common key management infrastructure. The use of open standards enables PKI to work with products from other vendors and simplifies its integration into existing networks.

PKI support also incorporates an open certificate architecture that provides the flexibility to customize user X.509 v3 certificates for many services and devices. This architecture enables organizations to add complementary products (connectors) that are designed to accept various certificate request types, so they can be used for Web browsers and servers, secure electronic transaction applications, and Virtual Private Network (VPN) devices and applications.

Secure Infrastructure

Nortel Networks has developed a portfolio of products that forms the network infrastructure to enable the secure transfer of health information. The following highlights the components of Nortel Networks Secure Infrastructure.

Optivity VPN Manager* (OVM)

VPN services may involve interconnection of multiple VPN access switches across wide geographic regions. Optivity VPN Manager provides VPN service administrators with an easy-to-use tool to manage the entire VPN service, supplying device-level details on multiple VPN switches from a single, network-wide management interface. The result is a more efficient and dependable VPN service for both enterprise and service provider customers.

Contivity Extranet Switch

Nortel Networks Contivity* Extranet switch product family provides the basis for a scalable, simple, and secure virtual private network (VPN) solution. Contivity Extranet switches serve as the secure entry point into the healthcare enterprise network, enabling access to the enterprise network anytime, anywhere, through a secure VPN. The Contivity Extranet switch integrates all of the necessary extranet technologies into a single platform — routing, firewall, bandwidth management, encryption, authentication, and data integrity via secure, standards-based (IPSec, PPTP, L2TP) tunneling and encryption across the Internet.

Passport Multi-Service Switches

Nortel Networks Passport* products are scalable, multi-service access edge switches which provide traffic aggregation for multiple traffic types, including circuit switched voice and video, SNA data, virtual circuits (frame relay and ATM) as well as IP traffic. Passport's Multiple Virtual Routing* (MVR) feature provides scalable, secure IP tunnels for VPNs with guaranteed quality of service. Passport products support NetSentry* advanced packet filtering, full firewall and network address translation (NAT) capabilities as part of its security capabilities. IPSec and PKI management are also supported.

BayStack Instant Internet

The BayStack* Instant Internet products are designed to quickly and easily connect smaller healthcare organizations to the Internet and provide secure VPN support. The easy-to-use software interface provides a unique, automated way for businesses to set up, manage, and control Internet access. For small and medium size healthcare organizations, Instant

Internet products provide cost-effective Internet connectivity. For larger organizations employing the Contivity Extranet Switch, VPN connectivity is easily established by adding an Instant Internet device at the branch office, allowing both remote and branch access at the host site.

Conclusion

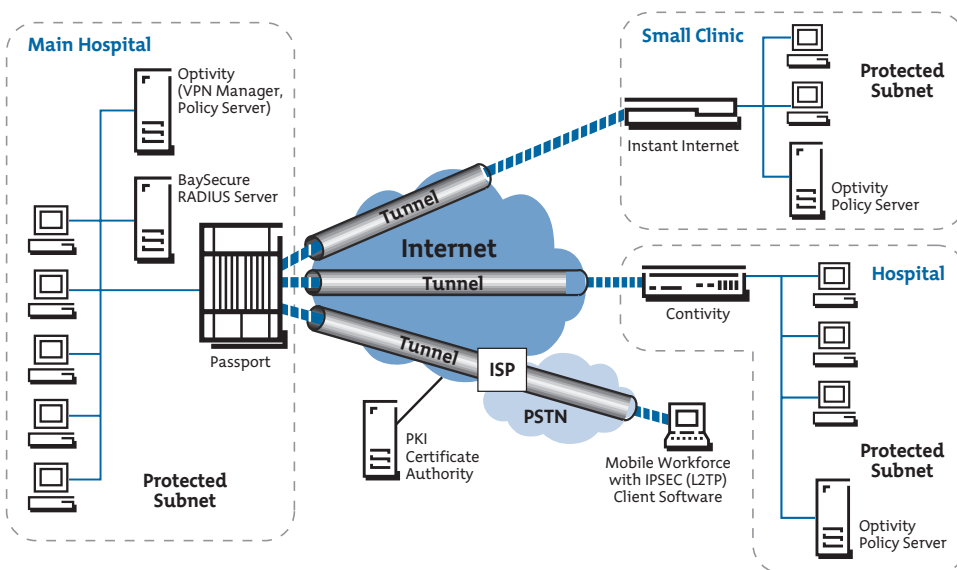
The overall goal for healthcare organizations is to implement a comprehensive, distributed security solution that adheres to both current and future healthcare legislation, allows for flexible and easy evolution over time, and minimizes the resulting impact this security infrastructure will have in terms of administrative personnel and network overhead. Nortel Networks' Security Solutions portfolio meets these goals by providing a structured solutions approach to securing healthcare networks.

Hypothetical Case Study—Celebrity Hospital Group

Celebrity Hospital Group (CHG) is an integrated delivery network comprising of two main hospitals, one clinic and healthcare providers working remotely. As they plan for comprehensive electronic data management, the CIO and the newly appointed security officer of CHG are faced with complying with the regulations, while preserving the delivery of quality healthcare.

CHG employs a number of patient data systems spread across several geographic locations. Some departments have begun to review their security practices in anticipation of the regulations, while others have not. Application vendors for the admission and discharge system, the lab order and reporting system and the Master Patient Database have stated their compliance to regulation. Currently, none of the vendors are responsible for ensuring that patient data is protected during transmission.

Figure 2: Celebrity Health Group's Secure Network.



Nortel Networks Security Solutions enables CHG's staff to meet the challenges of their diverse vendor environment and accelerating regulatory requirements, without increasing operational burdens. Through its capabilities, this security suite controls and monitors user access to any network-based enterprise application that "touches" patient data.

Nortel Networks Security Solution is composed of three solution "layers" that the CIO of CHG has drawn upon on to meet CHG's security requirements:

- Professional Security Assessment Services
- Authentication & Security Policy Management Technology
- Secure Network Infrastructure

Starting with the Right Partners

Meeting the challenges of responding to the regulations begins with an assessment of the security of the network and application environment. Nortel Networks, in collaboration with CHG security consultants and Nortel Networks security solution partners, carried out a security assessment to pinpoint security risks, and outline the options for creating a secure healthcare enterprise. Upon

completion of the security assessment, a network security policy and plan was crafted, and a secure VPN (employing a reliable national ISP) was proposed as the optimal network to connect CHG sites together.

Securing the Healthcare Network

The Nortel Network Security Solution, as applied to CHG's network, is shown in Figure 2. For the main CHG hospital, a Passport switch has been deployed as a high-capacity VPN access device, allowing multi-service traffic (voice, video, data) to be consolidated over the VPN. At the other CHG hospital as well as the clinic site, a Contivity Switch, acting as a security gateway, edge router and firewall has been deployed. This allows the individual sites to connect to the main hospital via secure IP tunnels over the Internet. The Contivity switches and the Passport are configured to use the IPSec standard, employ X.509 digital certificates for authentication, and Triple-DES for strong bulk data encryption. The firewall capabilities of Contivity help to assure that only authorized users are allowed

network access based on the hardware addresses of their systems, eliminating the threat of intruders connecting from unknown client devices.

In addition, all Contivity switches at each of the sites are managed by a single Optivity VPN Manager, located at the main hospital site, which allows simple configuration of all switches as well as VPN definition. Remote healthcare practitioners, working from home or in remote offices, employ the secure dial-up support on Contivity, in conjunction with IPSec client software running on their remote computers. This enables the remote users to establish secure connections to the main hospital, even though the transmission is taking place over the Internet.

Security policy management is provided via the Contivity switch according to user security profiles defined on the BaySecure RADIUS Server. This configuration allows appropriate hospital staff to have access to medical data, based on a need-to-know basis, thus reducing the chances for information breaches by unauthorized staff. User access is dynamically granted or refused, and can be restricted by application, department, user, or any combination of the three. BaySecure RADIUS audit capabilities allow CHG IT staff to review usage of network resources on demand by users, should they need to review any activity on the network for security reasons.

The identity of specific individuals accessing the main hospital network remotely is confirmed, and network access authorized (or denied) based on the identity of the user. The users' identity is determined by the Contivity Switches in conjunction with the PKI Certificate Authority, which transmits user authorization information to the hospital network in the form of a X.509 digital certificate.

Extending CHG's Network to its Partners

The Nortel Networks secure network implementation guarantees that the existing CHG sites can securely and cost-effectively connect together to exchange sensitive medical information, meeting the requirements of their security policy as well as HIPAA. However, this VPN solution also enables Celebrity

Health Group to extend beyond the reach of its' private Intranet by leveraging the ubiquity of the Internet and other IP-based public networks to link to other partners. This presumes that partner organizations have deployed secure VPN technology based on the same standards, including IPSec and X.509 digital certificates.

Celebrity Health Group can easily create, remove and maintain VPN extensions (otherwise known as CHG's "extranet") to their private network as required to communicate with new and changing healthcare business partners. Regardless of where the VPN is extended, traffic securely traverses the network with the help of tunneling and encryption technologies provided by the Nortel Networks Security Solution.



For more sales and product information, please call your account representative or 1-800-4-NORTEL.

United States

Nortel Networks
4401 Great America Parkway
Santa Clara, CA 95054
1-800-822-9638

Canada

Nortel Networks
8200 Dixie Road
Brampton, Ontario
L6T 5P6, Canada
1-800-466-7835

Europe, Middle East, and Africa

Nortel Networks
Les Cyclades - Immeuble Naxos
25 Allée Pierre Ziller
06560 Valbonne France
33-4-92-96-69-66

Asia Pacific

Nortel Networks
151 Lorong Chuan
#02-01 New Tech Park
Singapore 556741
65-287-2877

Caribbean and Latin America

Nortel Networks
1500 Concord Terrace
Sunrise, Florida
33323-2815 U.S.A.
954-851-8000

<http://www.nortelnetworks.com/health>

*Nortel Networks, the Nortel Networks logo, the Globemark, How the World Shares Ideas, BayRS, BaySecure, BayStack, Contivity, Entrust, Global Professional Services, Multiple Virtual Routing, NetID, NetSentry, Optivity, Optivity VPN Manager, Passport, and PKI are trademarks of Nortel Networks. All other trademarks are the property of their owners. © 2000 Nortel Networks. All rights reserved. Information in this document is subject to change without notice. Nortel Networks assumes no responsibility for any errors that may appear in this document. Printed in USA.