



HIPAA Readiness Using NetIQ Security and Administration Products to Ensure HIPAA Compliance

March 25, 2002

Contents

HIPAA Overview.....	1
NetIQ Products Offer a HIPAA Solution.....	2
HIPAA Requirements	3
How NetIQ Security Products Can Help.....	5
How NetIQ Administration Products Can Help	8
Conclusion.....	10
Links to HIPAA Resources	10

This document provides an overview of how NetIQ products help you plan for and maintain compliance with the security guidelines of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Tables summarize how specific NetIQ products satisfy individual requirements from the HIPAA regulations. NetIQ products can help you comply with requirements from all four categories of the security regulations.

With these NetIQ products, you can meet your HIPAA-compliance goals while streamlining your business processes and reducing your overall costs of doing business.

THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT ARE FURNISHED UNDER AND ARE SUBJECT TO THE TERMS OF A LICENSE AGREEMENT OR A NON-DISCLOSURE AGREEMENT. EXCEPT AS EXPRESSLY SET FORTH IN SUCH LICENSE AGREEMENT OR NON-DISCLOSURE AGREEMENT, NETIQ CORPORATION PROVIDES THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW DISCLAIMERS OF EXPRESS OR IMPLIED WARRANTIES IN CERTAIN TRANSACTIONS; THEREFORE, THIS STATEMENT MAY NOT APPLY TO YOU.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of NetIQ Corporation, except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of NetIQ Corporation. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. NetIQ Corporation may make improvements in or changes to the software described in this document at any time.

© 1995-2002 NetIQ Corporation, all rights reserved.

U.S. Government Restricted Rights: If the software and documentation are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), in accordance with 48 C.F.R. 227.7202-4 (for Department of Defense (DOD) acquisitions) and 48 C.F.R. 2.101 and 12.212 (for non-DOD acquisitions), the government's rights in the software and documentation, including its rights to use, modify, reproduce, release, perform, display or disclose the software or documentation, will be subject in all respects to the commercial license rights and restrictions provided in the license agreement.

ActiveAgent, ActiveAnalytics, ActiveKnowledge, ActiveReporting, ADcheck, AppAnalyzer, Application Scanner, AppManager, AuditTrack, AutoSync, Chariot, Chariot VoIP Assessor, ClusterTrends, CommerceTrends, Configuration Assessor, ConfigurationManager, the cube logo design, DBTrends, DiagnosticManager, Directory and Resource Administrator, Directory Security Administrator, Domain Migration Administrator, End2End, Exchange Administrator, Exchange Migrator, Extended Management Pack, FastTrends, File Security Administrator, Firewall Appliance Analyzer, Firewall Reporting Center, Firewall Suite, Ganymede, the Ganymede logo, Ganymede Software, Group Policy Administrator, Intergreat, Knowledge Scripts, Log Analyzer, Migrate.Monitor.Manage, Mission Critical Software, Mission Critical Software for E-Business, the Mission Critical Software logo, MP3check, NetIQ, the NetIQ logo, the NetIQ Partner Network design, NetWare Migrator, OnePoint, the OnePoint logo, Operations Manager, Qcheck, RecoveryManager, Security Analyzer, Security Manager, Server Consolidator, SQLcheck, Visitor Mean Business, Visitor Relationship Management, VoIP Manager, W logo, WebTrends, WebTrends Analysis Suite, WebTrends Data Collection Server, WebTrends for Content Management Systems, WebTrends Intelligence Suite, WebTrends Live, WebTrends Network, WebTrends OLAP Manager, WebTrends Report Designer, WebTrends Reporting Center, WebTrends Warehouse, Work Smarter, WWWorld, and XMP are trademarks or registered trademarks of NetIQ Corporation or its subsidiaries in the United States and other jurisdictions. All other company and product names mentioned are used only for identification purposes and may be trademarks or registered trademarks of their respective companies.

HIPAA Overview

Health care organizations that maintain electronic patient information must ensure the privacy and confidentiality of that information by complying with regulations from the U. S. Department of Health and Human Services (HHS). NetIQ security and administration products help health care organizations comply with these regulations.

What Is HIPAA?

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 places comprehensive new security requirements on the health care industry. Sometimes dubbed the *Y2K of health care*, HIPAA imposes sweeping standards for the privacy and protection of all electronic health information that can be linked to individuals. HHS is publishing final HIPAA regulations that affect virtually every area of health-related organizations in the United States, from the one-physician office to multi-entity health systems, HMOs, health care support services, and others. If you work in the health care industry, you must comply with these security regulations, in most cases, by April 14, 2003. Non-compliance will carry stiff civil and criminal penalties.

Who Is Affected?

All health care organizations are affected in some way by HIPAA. The entities that are affected include all health care providers (even one-physician offices), health plans, employers, public health authorities, hospitals, life insurers, clearinghouses, billing agencies, information systems vendors, service organizations, and universities.

Are There Penalties for Noncompliance?

HIPAA calls for severe civil and criminal penalties for noncompliance, including:

- Fines up to \$25,000 for multiple violations of the same standard in a calendar year
- Fines up to \$250,000 and/or imprisonment up to 10 years for known misuse of individually identifiable health information

What about Costs?

Some have estimated that HIPAA compliance will consume 33 cents of every health care dollar spent between now and the end of 2002. No one knows what the actual costs will be, and the costs will vary widely depending on your type of business and the type of information your organization handles electronically. The advantage to you, despite these costs, is that by complying with HIPAA regulations, your organization should gain streamlined processes and reduced risks of losing or compromising valuable patient information. The overall, long-term effect to your organization of complying with HIPAA regulations should be to reduce your costs for information management.

NetIQ Products Offer a HIPAA Solution

Four categories of requirements for safeguarding patient information comprise the HIPAA security standard:

- Administrative Procedures
- Physical Safeguards
- Technical Security Services
- Technical Security Mechanisms

NetIQ Security Manager, NetIQ Security Analyzer, Firewall Reporting Center, and the NetIQ administration products help with HIPAA compliance by comprehensively assessing health organizations' information security systems, policies, and procedures. NetIQ products take away the pain of implementing HIPAA in an enterprise network. Security Manager and the administration products make the task of implementing comprehensive action plans, including developing new policies, processes, and procedures, simple. NetIQ Corporation has made it possible to leverage your current security investment by integrating your purchased tools into Security Manager, giving you a single, simple *View* into your corporate security systems. NetIQ products provide the following features:

- Consolidation of event logs, giving you the ability to audit your systems in a timely fashion. This consolidation also gives you the ability to correlate events that may be crucial to have a complete security solution.
- Audit reports that will get your organization ready for an external audit.
- Intrusion detection that allows you to know who or what is trying to access your systems and block those intruders from access to vital information.
- Firewall monitoring and firewall policy reporting throughout your organization.
- Detection of all security risks on individual servers throughout your enterprise and re-evaluation of those risks on a regular basis.
- Protection of your enterprise from internal and external attacks on important and confidential information.
- Extensive reporting that allows you to track unauthorized changes to hardware, software, or access permissions and take appropriate actions.
- Monitoring the current state of your environment and alerting you to potential security violations.
- Control over your network security model through advanced delegation and powerful, policy-based management capabilities.
- Identification of potential security holes in your network configuration, file systems, printer configurations, and shares.
- Secure management of access control lists (ACLs) in the Active Directory.
- Highly secure administration for Windows NT 4, Windows 2000 and the Active Directory, Exchange 5.5, Exchange 2000, and Windows resources, such as printers, shares, and file systems.
- Delegation and automation of time-consuming administrative tasks to ensure efficient and consistent application security across the network.
- Help for closely managing user accounts, groups, service accounts, and resources.

HIPAA Requirements

NetIQ security and administration products provide much of the support you need to show compliance with HIPAA regulations. NetIQ Security Manager, NetIQ Security Analyzer, Firewall Reporting Center products enable you to enforce security policies, monitor for security breaches, and reduce vulnerabilities in your network. The NetIQ Administration Suite products enable you to control access to network resources, enforce security policies, and provide audit trails through extensive reporting capabilities.

This document includes information about the following NetIQ products:

- Security Manager
- Security Analyzer
- Firewall Reporting Center
- Directory and Resource Administrator (DRA)
- Directory Security Administrator (DSA)
- File Security Administrator (FSA)
- Configuration Assessor (CA)
- Group Policy Administrator (GPA)

NetIQ products can help you comply with requirements from all four categories of the security regulations. The following sections summarize which NetIQ products address specific requirements of the HIPAA security regulations. Since the Technical Security Services and Technical Security Mechanisms requirements are closely related, they are discussed together in one section.

HIPAA Requirement: Administrative Procedures

The Administrative Procedures deal with defining and implementing a security policy for keeping information private. The following table outlines the NetIQ products that help with administrative procedures.

HIPAA Requirement	NetIQ Products to Address Requirement
Certification and application analysis	DRA, DSA, FSA, CA, GPA
Disaster and emergency plan	DRA
Information access control	DRA, DSA, FSA, GPA, Security Manager
Access audits	Security Manager
Configuration management	DRA, CA, GPA, Security Manager, Security Analyzer, Firewall Reporting Center
Security incident	DRA, DSA, CA, GPA, Security Manager
Security management	DRA, DSA, FSA, CA, GPA, Security Manager
Termination procedures	DRA, DSA, FSA

HIPAA Requirement: Physical Safeguards

The Physical Safeguards deal with methods you use to protect data. The following table outlines the NetIQ products that help with physical safeguarding of data.

HIPAA Requirement	NetIQ Products to Address Requirement
Assigned security	DRA, DSA, FSA, CA
Media controls	DRA, DSA, FSA, GPA
Physical access controls	DRA

HIPAA Requirements: Technical Security Services and Technical Security Mechanisms

Technical Security Services and Technical Security Mechanisms deal with the methods you use for securing data access. The following table outlines the NetIQ products that help with technical security services and mechanisms.

HIPAA Requirement	NetIQ Products to Address Requirement
Access controls	DRA, DSA, FSA, GPA
Audit controls	DRA, DSA, FSA, CA, Security Manager
Authorization controls	DRA, FSA
Entity authentication	DRA, FSA, Security Manager, Security Analyzer
Network controls	Security Manager

How NetIQ Security Products Can Help

The NetIQ security products provide the following benefits for HIPAA compliance:

- Reduce exposure to vulnerabilities
- Identify potential areas for compromise
- Improve audit performance
- Consolidate event logs
- Monitor real time security
- Detect new computers on the network
- Create extensive reports
- Ensure company confidentiality
- Protect intellectual property from theft
- Preserve *trail of evidence*
- Reduce number of security incidents
- Give a real-time security view into the enterprise
- Offer a centralized security console
- Identify resources out of compliance with established policies
- Integrate with existing third-party security solutions

NetIQ Security Manager, NetIQ Security Analyzer, and Firewall Reporting Center products enable you to show compliance with the Administrative Procedures, Technical Security Services, and Technical Security Mechanisms sections of the HIPAA regulations. The following sections provide more details about the features of NetIQ security products that relate to HIPAA compliance.

Intrusion Detection Capabilities

Security Manager offers continuous monitoring and notification of breaches to your network security. The following details show how Security Manager helps you protect patient information:

- Protects against denial of service attacks
 - Automatically denies an offending host access to the Web server by inserting the IP address into the **Deny IP** field of IIS computers
 - Monitors Exchange mailboxes for possible incoming, harmful email viruses
- Detects improper use of service accounts
 - Detects when a service account is used for interactive logon and automatically logs off the user
- Detects rogue processes
 - Uses inclusive method, where user defines list of acceptable processes
 - Uses exclusive method, where user defines list of unacceptable processes
- Detects logon violations
 - Correlates failed logon events and alerts when suspicious failed logon events occur

Event Log Consolidation

Security Manager streamlines your administrative procedures by consolidating event logs in real time. Security Manager helps you investigate security incidents by managing event log entries:

- Stores event log entries in a centralized repository
- Prevents intruders from covering tracks by clearing logs
- Maintains chain of custody for evidence purposes
- Forwards UNIX, router, and switch logs through the syslog for correlation with other events
- Stores logs from custom applications that use the clear text log format
- Relocates logs located on servers in DMZs and extranets to shield sensitive information from unauthorized access

Automated Security Policy Enforcement

Security Manager allows you to automate security policy enforcement. Its reporting provides much of the documentation required to substantiate security policy compliance. Security Manager automates security policy enforcement in the following ways:

- Automatically deploys configuration policies to resources and new computers
- Automates auditing of resources to ensure compliance with policy
- Provides knowledge of known security issues
- Integrates with other NetIQ products to restore security policies on resources that are out of compliance

Incident Resolution Workflow Management

When a security incident occurs, you need the right person to be able to respond to the incident. Security Manager helps you resolve incidents in several ways:

- Provides historical tracking, state management, customizable knowledge base, and Web article URL links
- Allows customized views of service-level exceptions (alerts not being processed through the organization as directed)
- Provides customized consoles and Web portals so each user can quickly view only the information needed
- Notifies by email and paging
- Runs scripts to automatically respond in a standard way

Security Manager as Guardian

Security Manager provides automated responses to protect your environment:

- Disables unauthorized user accounts
- Terminates unauthorized processes
- Identifies unauthorized ports
- Logs off users who do not comply with security policy
- Backs up event logs to maintain audit trails
- Creates Emergency Repair Disks and stores them in a central location
- Denies unauthorized access to Web servers
- Enforces security configuration policies

Vulnerability Assessment

When preparing for and maintaining compliance with HIPAA regulations, you must be able to assess the vulnerabilities in your environment. Security Analyzer and Security Manager check for security vulnerabilities using the following methods:

- Verifies that the latest security patches have been applied
- Checks password strength and report weak passwords
- Verifies that backdoors are closed
- Scans ports for vulnerabilities
- Identifies resources that do not comply with security configuration policy
- Scans network for common known vulnerabilities

Virus Detection

Security Manager provides knowledge for McAfee, Norton, and Trend Micro virus detection software and helps maintain a virus-free environment using the following methods:

- Sends instant notification when viruses are detected on sensitive file servers
- Generates alerts when a server has a virus that cannot be cleaned by the antivirus software
- Takes corrective action if the antivirus software is disabled
- Notifies administrator when signature file has not been updated in a specified number of days
- Uses a dedicated Exchange mailbox and notifies appropriate personnel when a potential email virus enters the mailbox

Enterprise-Wide Firewall Configuration Management

According to the International Computer Security Association (ICSA), 70 percent of firewalls are vulnerable to attack due to configuration or improper deployment. Security Manager and Firewall Reporting Center help you manage firewalls in the following ways:

- Set desired configuration policies
- Automatically correct policy violations
- Identify firewall events and external attacks in real-time
- Provide automatic alert notification
- Provide single point for firewall monitoring, management, and consolidated event repository
- Provide knowledge base that includes pre-configured automated responses
- Integrate with more than 35 popular firewalls

Audit Readiness Reports

Reports help with your initial planning of security policies and with your audit requirements after implementing security policies. Security Manager provides extensive reporting that you can use to show readiness and compliance with HIPAA security regulations:

- Provides customers with security audit reports
- Sends patch status across the enterprise
- Highlights password issues
- Tracks file security changes
- Tracks remote access usage
- Reports security log attributes and activity
- Reports user account trends and anomalies
- Tracks domain policy changes

How NetIQ Administration Products Can Help

The NetIQ administration products provide the following benefits for HIPAA compliance:

- Provide highly secure administration for all networks
- Reduce exposure to unauthorized network changes
- Identify areas where security can be strengthened
- Delegate administration tasks to put people who know in charge
- Enable powerful auditing capabilities
- Control network access through policy enforcement
- Create extensive reports to monitor changes to permissions or resources
- Back up and restore permissions
- Ensure company confidentiality
- Protect intellectual property from theft
- Preserve *trail of evidence*
- Offer a centralized administration console
- Identify resources out of compliance with established policies
- Integrate with native operating system tools

NetIQ administration products enable you to show compliance with the Administrative Procedures, Physical Safeguards, Technical Security Services, and Technical Security Mechanisms categories of the HIPAA security regulations.

The NetIQ products discussed in the following sections include:

- Directory and Resource Administrator (DRA)
- Directory Security Administrator (DSA)
- File Security Administrator (FSA)
- Configuration Assessor (CA)
- Group Policy Administrator (GPA)

The following sections provide more details about the features of NetIQ administration products that relate to HIPAA compliance.

Resource Management

NetIQ administration products provide highly secure administration for your Windows resources, such as printers, shares, and file systems. DRA, DSA, FSA, CA, and GPA are part of an integrated suite of products that eliminates the problems of deploying products from multiple vendors. These products help you manage resources in the following ways:

- Provide reporting, event logging, and security model management
- Assess computer configurations
- Search for file permissions and determine who can access what
- Search for Active Directory permissions and determine resultant permissions
- Generate and maintain group policy objects
- Provide multi-master model for continued operation should one administration server fail

Access Control

DRA, DSA, FSA, and GPA provide secure and automated management of your environment. NetIQ administration products help you manage information access in the following ways:

- Manage Active Directory permissions for user accounts, groups, and computer accounts
- Manage Windows NT user accounts and groups
- Manage file and folder permissions throughout the file system
- Standardize group policy administration
- Give a current state view of your file systems and allow you to quickly take corrective action

Configuration Management

CA reports essential details about your environment and helps you improve your administration process. This assessment and reporting tool for Windows NT 4, Windows 2000/Active Directory and Exchange servers provides you with reports detailing a variety of information, including hardware configuration and potential security holes. CA assists with configuration management in the following ways:

- Review hardware and software installations for compliance with group policy
- Report on storage usage
- Check for security violations

Risk Analysis and Management

DSA, FSA, CA, and GPA help you create, administer, and oversee policies that prevent, detect, contain, and correct security breaches. These administration products help you apply risk analysis and management in the following ways:

- Report potential security holes
- Search for unauthorized Active Directory access permissions
- Ensure compliance with group policy
- Analyze computer configurations
- Identify inappropriate file permissions and help you restore and maintain appropriate permissions

Authorization Control

DRA and FSA help to ensure that only properly authorized individuals can access health information in your environment. These products secure authorization control in the following ways:

- Provide a role-based security model
- Eliminate and prevent enterprise security holes
- Give you a view of the current state of your file systems and allow you to quickly take corrective action

Audit Control

DRA, DSA, FSA and CA provide audit control mechanisms to record and examine system activity. These products provide the following audit controls:

- Log all actions in detail and provide extensive security reporting for resources
- Report on permission changes in the Active Directory
- Report on file and folder permissions
- Backup and restore appropriate permissions
- Report on computer configurations

Conclusion

The NetIQ security products offer the most comprehensive solutions to secure network information. These products keep your data secure, allow administrators to take action against would-be intruders, report violations in an easy-to-use format, monitor systems for security vulnerabilities, enforce set policies, monitor firewall changes, and make it easy for security administrators to review their network from a centralized security view.

The NetIQ administration products provide the best management and analysis products for your environment. These products automate administration tasks to avoid costly mistakes, enforce policies to maintain your security model, secure data on the network, report changes to permissions, analyze computer configurations and permissions, and automate group policy management.

With these NetIQ products, you can meet your HIPAA-compliance goals while streamlining your business processes and reducing your overall costs of doing business.

Links to HIPAA Resources

The following Web sites contain detailed information related to HIPAA regulations and compliance.

Department of Health and Human Services (HHS) – aspe.os.dhhs.gov/admnsimp

This comprehensive HIPAA site is the official source for information on regulations published by HHS. You can download or print the proposed regulations and public comments from this site.

Main HCFA HIPAA page – www.hcfa.gov/hipaa/hipaahm.htm

This site contains information about how the Health Care Financing Administration (HCFA) is responsible for implementing various unrelated provisions of HIPAA.

Designated Standard Maintenance Organizations (DSMOs) – www.hipaa-dsmo.org

This site contains FAQs and procedures for requesting a change to HIPAA standards.

Center for Internet Security – www.cisecurity.org

This site contains information to help organizations effectively manage the risks related to information security. CIS provides methods and tools to improve, measure, monitor, and compare the security status of your Internet-connected systems and appliances.

Health Data Management – www.healthdatamanagement.com

This site contains stories from *Health Data Management* magazine and includes an area devoted to HIPAA-related press releases and news stories.