



HIPAA Security Matrix

White Paper

April 8, 2002

Contents

Introduction to HIPAA.....	1
Understanding the Security Matrix	1
Administrative Procedures	2
Physical Safeguards	9
Technical Security Services.....	11
Technical Security Mechanisms	13

This document provides a summary of the HIPAA guidelines and which NetIQ products help you comply with these guidelines. This extensive list covers more than 20 specific areas that require policies and procedures in place to insure the integrity, availability, and security of protected health information.

The government has intentionally left undefined the level to which each of these areas needs to be addressed. Each organization must review its exposure, risk, and cost of compliance and set its own level of compliance. For example, a two-person business has a much different risk versus benefit analysis than a 400 bed hospital. HIPAA leaves the specifics of compliance up to each individual organization.

Legal Notice

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: The software and the documentation are commercial computer software and documentation developed at private expense. Use, duplication, or disclosure by the Government is subject to the terms of the NetIQ standard commercial license for the software, and where applicable, the restrictions set forth in the Rights in Technical Data and Computer Software clauses and any successor rules or regulations.

ActiveAgent, ActiveEngine, ActiveKnowledge, ADcheck, AppAnalyzer, Application Scanner, AppManager, the AppManager logo, AutoSync, Chariot, Configuration Assessor, ConfigurationManager, DiagnosticManager, Directory and Resource Administrator, Directory Security Administrator, Domain Migration Administrator, End2End, Enterprise Administrator, Exchange Administrator, Exchange Migrator, File Security Administrator, Ganymede, Ganymede Software, the Ganymede logo, Knowledge Pack, Knowledge Scripts, Mission Critical Software, the Mission Critical Software logo, MP3check, NetIQ, the NetIQ logo, NetIQ Partner Network, the NetIQ Partner Network logo, NetWare Migrator, OnePoint, the OnePoint logo, Operations Manager, Pegasus, Qcheck, RecoveryManager, Security Analyzer, Security Manager, Server Consolidator, SQLcheck, WebTrends, Work Smarter, 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.

Introduction to HIPAA

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). 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. The specific requirements for guarding data integrity, confidentiality, and availability fall into four categories:

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

Organizations must comply with these security regulations, in most cases, by April 14, 2003. Non-compliance will carry stiff civil and criminal penalties.

NetIQ security and administration products help health care organizations comply with these regulations. This document provides a security matrix that matches NetIQ product features with the HIPAA requirement each feature satisfies.

Understanding the Security Matrix

Each of the following sections identifies a category of requirements for guarding data integrity, confidentiality, and availability within the HIPAA guidelines.

Within these sections, a table identifies the requirement and implementation portions of the HIPAA guidelines that apply to the associated category. The tables also identify the NetIQ products and features that help you comply with each requirement.

For an explanation of each specific requirement in the tables, see the following links:

Administrative Procedures

aspe.os.dhhs.gov/admnsimp/nprm/sec06.htm

Physical Safeguards

aspe.os.dhhs.gov/admnsimp/nprm/sec07.htm

Technical Security Services

aspe.os.dhhs.gov/admnsimp/nprm/sec08.htm

Technical Security Mechanisms

aspe.os.dhhs.gov/admnsimp/nprm/sec09.htm

Administrative Procedures

Requirement	NetIQ Product and Feature	Notes
Certification	DRA: Provides detailed reports, improves auditing through event logs, and standardizes security model DSA: Manages and analyzes Active Directory ACLs FSA: Manages all aspects of permissions throughout the file system GPA: Manages all aspects of group policy CA: Manages computer configuration assessment	
Chain of trust partner agreement		

Requirement	NetIQ Product and Feature	Notes
Contingency plan:		All listed features of this requirement must be implemented.
<ul style="list-style-type: none"> • Applications and data criticality analysis 	<p>DRA: Provides detailed reports, improves auditing through event logs, and standardizes security model</p> <p>FSA: Allows searching and reporting on permissions throughout the file system</p> <p>CA: Provides computer configuration assessment</p> <p>DSA: Allows searching and reporting on ACL settings throughout the Active Directory</p> <p>GPA: Generates and maintains group policy</p>	
<ul style="list-style-type: none"> • Data backup plan 	<p>FSA: Backs up and restores file and folder permissions</p> <p>GPA: Backs up and restores group policies</p>	
<ul style="list-style-type: none"> • Disaster recovery plan 	<p>DRA: Provides multi-master model for security replication should one Administration server fail</p> <p>FSA: Backs up and restores file and folder permissions</p> <p>GPA: Backs up and restores group policies</p> <p>Security Manager: Stores components on multiple computers, with buffering for guaranteed delivery</p>	
<ul style="list-style-type: none"> • Emergency mode operation plan 	<p>DRA: Provides multi-master model for continued operation should one Administration server fail</p>	
<ul style="list-style-type: none"> • Testing and revision 		
Formal mechanism for processing records		

Requirement	NetIQ Product and Feature	Notes
Information access control:		All listed features of this requirement must be implemented.
<ul style="list-style-type: none"> • Access authorization 	<p>DRA: Manages Active Directory resources, Windows NT user accounts and groups, and standardizes security model</p> <p>DSA: Manages and analyzes Active Directory ACLs</p> <p>FSA: Manages all aspects of permissions throughout the file system</p> <p>GPA: Manages all aspects of group policy</p> <p>Security Manager: Allows people to manage security only in their area, limiting data they see</p>	
<ul style="list-style-type: none"> • Access establishment 	<p>DRA: Offers a secure, three-tier architecture, creating a protected business layer between the end user and the managed data</p>	
<ul style="list-style-type: none"> • Access modification 	<p>DRA: Manages Active Directory resources, Windows NT user accounts and groups, and standardizes security model</p> <p>DSA: Manages and analyzes Active Directory ACLs</p> <p>FSA: Manages all aspects of permissions throughout the file system</p> <p>GPA: Manages all aspects of group policy</p>	
Internal audit		

Requirement	NetIQ Product and Feature	Notes
Personnel security:		All listed features of this requirement must be implemented.
<ul style="list-style-type: none"> • Assure supervision of maintenance personnel by authorized, knowledgeable person 		
<ul style="list-style-type: none"> • Maintenance of record of access authorizations 	Security Manager: Provides event collection to keep record of logins, file access, and security	
<ul style="list-style-type: none"> • Operating, and in some cases, maintenance personnel have proper access authorization 		
<ul style="list-style-type: none"> • Personnel clearance procedure 		
<ul style="list-style-type: none"> • Personnel security policy/procedure 		
<ul style="list-style-type: none"> • System users, including maintenance personnel trained in security 		

Requirement	NetIQ Product and Feature	Notes
Security configuration management:		All listed features of this requirement must be implemented.
<ul style="list-style-type: none"> • Documentation 		
<ul style="list-style-type: none"> • Hardware/software installation and maintenance review and testing for security features 	DRA: Provides resource management CA: Provides computer configuration analysis GPA: Provides Group Policy Object definition for good practices throughout the network	
<ul style="list-style-type: none"> • Inventory 	CA: Provides detailed reports on computer configurations	
<ul style="list-style-type: none"> • Security testing 	Security Manager: Provides vulnerability assessment for security policy Security Analyzer: Provides vulnerability assessment for multiple operating systems Firewall Reporting Center: Provides vulnerability assessment for firewalls	
<ul style="list-style-type: none"> • Virus checking 	Security Manager: Provides antivirus module	
Security incident procedures:		All listed features of this requirement must be implemented.
<ul style="list-style-type: none"> • Report procedures 	Security Manager: Provides knowledge bases and reporting DRA: Provides detailed resource reporting DSA: Provides reporting on Active Directory ACLs CA: Provides reporting on computer configurations GPA: Provides detailed reporting on group policy	
<ul style="list-style-type: none"> • Response procedures 	Security Manager: Provides knowledge bases and automated responses	

Requirement	NetIQ Product and Feature	Notes
Security management process:		All listed features of this requirement must be implemented.
<ul style="list-style-type: none"> • Risk analysis 	<p>DSA: Provides search and analysis of Active Directory permissions</p> <p>GPA: Provides group policy object analysis</p>	
<ul style="list-style-type: none"> • Risk management 	<p>DSA: Provides search and analysis of Active Directory permissions</p> <p>CA: Provides computer configuration analysis</p> <p>FSA: Allows searching and reporting on permissions throughout the file system</p> <p>GPA: Provides group policy object analysis</p>	
<ul style="list-style-type: none"> • Sanction policy 		
<ul style="list-style-type: none"> • Security policy 	<p>Security Manager: Provides security policy enforcement through security configuration management</p> <p>DRA: Provides policies and triggers to automate notification and responses</p> <p>GPA: Manages Group policy object definition for good practices throughout the network</p>	

Requirement	NetIQ Product and Feature	Notes
Termination procedures:		All listed features of this requirement must be implemented.
<ul style="list-style-type: none"> • Combination locks changed 		
<ul style="list-style-type: none"> • Removal from access lists 	<p>DRA: Manages Active Directory resources, Windows NT user accounts and groups, and standardizes security model</p> <p>DSA: Manages and analyzes Active Directory ACLs</p> <p>FSA: Manages all aspects of permissions throughout the file system</p>	
<ul style="list-style-type: none"> • Removal of user accounts 	<p>DRA: Provides Windows NT and Active Directory administration and Recycle Bin for user accounts</p>	
<ul style="list-style-type: none"> • Turn in keys, token, or cards that allow access 		
Training:		
<ul style="list-style-type: none"> • Awareness training for all personnel, including management 		All listed features of this requirement must be implemented.
<ul style="list-style-type: none"> • Periodic security reminders 		
<ul style="list-style-type: none"> • User education concerning virus protection 		
<ul style="list-style-type: none"> • User education in importance of monitoring log in success/failure, and how to report discrepancies 		
<ul style="list-style-type: none"> • User education in password management 		

Physical Safeguards

Requirement	NetIQ Product and Feature	Notes
Assigned security responsibility	<p>DRA: Manages Active Directory resources, Windows NT user accounts and groups, and standardizes security model</p> <p>FSA: Allows searching and reporting on permissions throughout the file system</p> <p>CA: Provides computer configuration assessment</p> <p>DSA: Allows searching and reporting on ACL settings throughout the Active Directory</p>	
Media controls:		All listed features of this requirement must be implemented.
<ul style="list-style-type: none"> • Access control 	<p>DSA: Allows searching and modifying directory-controlled access to files and network resources</p> <p>GPA: Automates group policy management to lock down desktop and server configurations</p> <p>FSA: Allows searching and reporting on permissions throughout the file system</p>	
<ul style="list-style-type: none"> • Accountability (tracking mechanism) 	<p>DRA: Provides detailed reports and improves auditing through event logs</p>	
<ul style="list-style-type: none"> • Data backup 		
<ul style="list-style-type: none"> • Data storage 		
<ul style="list-style-type: none"> • Disposal 		

Requirement	NetIQ Product and Feature	Notes
Physical access controls (limited access):		All listed features of this requirement must be implemented.
<ul style="list-style-type: none"> • Disaster recovery 	DRA: Provides multi-master model for security replication should one Administration server fail	
<ul style="list-style-type: none"> • Emergency mode operation 	DRA: Provides multi-master model for continued operation should one Administration server fail	
<ul style="list-style-type: none"> • Equipment control (into and out of site) 		
<ul style="list-style-type: none"> • Facility security plan 		
<ul style="list-style-type: none"> • Procedures for verifying access authorizations prior to physical access 		
<ul style="list-style-type: none"> • Maintenance records 		
<ul style="list-style-type: none"> • Need-to-know procedures for personnel access 		
<ul style="list-style-type: none"> • Sign-in for visitors and escort, if appropriate 		
<ul style="list-style-type: none"> • Testing and revision 		
Policy/guideline on work station use		
Secure work station location		
Security awareness training		

Technical Security Services

Requirement	NetIQ Product and Feature	Notes
Access control:		<p>The following feature must be implemented:</p> <ul style="list-style-type: none"> • Procedure for emergency access <p>In addition, at least one of the following features must be implemented:</p> <ul style="list-style-type: none"> • Context-based access • Role-based access • User-based access <p>The use of encryption is optional.</p>
• Context-based access		
• Encryption		
• Procedure for emergency access		
• Role-based access	<p>DRA: Manages security model administration</p> <p>FSA: Manages security model administration</p> <p>GPA: Manages group policy administration</p>	
• User-based access	<p>DRA: Manages security model administration</p> <p>FSA: Manages security model administration</p>	
Audit controls	<p>Security Manager: Provides event collection and reporting to keep record of logins, file access, and security</p> <p>DRA: Provides detailed resource reporting</p> <p>DSA: Provides reporting on Active Directory ACLs</p> <p>CA: Provides reporting on computer configurations</p> <p>FSA: Provides reporting on file and folder permissions throughout the file system</p>	

Requirement	NetIQ Product and Feature	Notes
Authorization control:		At least one of the listed features of this requirement must be implemented.
<ul style="list-style-type: none"> • Role-based access 	DRA: Manages security model administration FSA: Manages security model administration	
<ul style="list-style-type: none"> • User-based access 	DRA: Manages security model administration FSA: Manages security model administration	
Data authentication		
Entity authentication:		The following features must be implemented: <ul style="list-style-type: none"> • Automatic logoff • Unique user identification In addition, at least one of the other listed features of this requirement must be implemented.
<ul style="list-style-type: none"> • Automatic logoff 	Security Manager: Enforces through security configuration management	
<ul style="list-style-type: none"> • Biometric 		
<ul style="list-style-type: none"> • Password 	Security Manager: Enforces password policy Security Analyzer: Checks for weak passwords DRA: Enforces password policy	
<ul style="list-style-type: none"> • PIN 		
<ul style="list-style-type: none"> • Telephone callback 		
<ul style="list-style-type: none"> • Token 		
<ul style="list-style-type: none"> • Unique user identification 	DRA: Manages security model administration FSA: Manages security model administration	

Technical Security Mechanisms

Requirement	NetIQ Product and Feature	Notes
Communications/network controls:		<p>If communications or networking is employed, the following features must be implemented:</p> <ul style="list-style-type: none"> • Integrity controls • Message authentication <p>One of the following features must also be implemented:</p> <ul style="list-style-type: none"> • Access controls • Encryption <p>In addition, if using a network, the following features must be implemented:</p> <ul style="list-style-type: none"> • Alarm • Audit trail • Entity authentication • Event reporting
<ul style="list-style-type: none"> • Access controls 	FSA: Manages all aspects of permissions throughout the file system	
<ul style="list-style-type: none"> • Alarm, event reporting, and audit trail 	Security Manager: Provides automated responses to events	
<ul style="list-style-type: none"> • Audit trail 	Security Manager: Provides event collection to keep record of logins, file access, and security	
<ul style="list-style-type: none"> • Encryption 		
<ul style="list-style-type: none"> • Entity authentication 		
<ul style="list-style-type: none"> • Event reporting 	Security Manager: Provides event collection and reporting to keep record of logins, file access, and security	
<ul style="list-style-type: none"> • Integrity controls 		
<ul style="list-style-type: none"> • Message authentication 		