

NetIQ's Directory and Resource Administrator™ Helps Kindred Healthcare Comply with New HIPAA Regulations

Kindred Healthcare, one of the nation's most respected healthcare providers, uses NetIQ's Directory and Resource Administrator to help ensure separation of duties and proper information access and security for 20,000 users in its health system. Directory and Resource Administrator serves as Kindred's primary administrative and security support tool for assuring compliance with internal audit standards and HIPAA regulations for patient information privacy and confidentiality.



Executive Summary

Industry

Operating in more than 40 states, Kindred Healthcare provides healthcare through 260 skilled nursing centers, more than 60 long-term acute care hospitals and 30 institutional pharmacies. The company has grown through acquisition to rank among the top five long-term healthcare providers in North America.

Business Situation

Kindred's aggressive growth has been matched by its IT commitment to strict compliance with internal audit standards that in turn meet or exceed recent HIPAA regulations governing the use and protection of information collected and utilized by healthcare providers. Kindred's IT solution required a migration from Windows NT to Windows 2000 along with the development of an in-house user provisioning system to help manage 60,000 employees, 8,000 Windows desktops and more than 1,200

Windows servers. Directory and Resource Administrator from NetIQ was selected as its main security and administrative tool to help define and manage user roles and security in Active Directory.

Benefits

NetIQ's Directory and Resource Administrator provides an automated, easy to use solution that integrates with Kindred's in-house user provisioning application to ensure the separation of duties and enforce role based security policies. Directory and Resource Administrator helps reduce administrative costs and overhead while providing granular control and reporting to meet internal audit standards and comply with HIPAA regulations.

Products

NetIQ Directory and Resource Administrator

"It would be very difficult to live without NetIQ's Directory and Resource Administrator since it gives us the ability to ensure separation of duties, automate many manual processes and help us meet new HIPAA regulations all necessary to ensure the appropriate privacy and confidentiality of our patient information."

Kelley Ealy, Security Analyst, Kindred Healthcare

Ahead of the Game in Meeting New HIPAA Regulations

The security and privacy of patient information is top priority for Kindred's IT operations according to Kelley Ealy, security analyst. "We have very strong internal audit and security standards," she emphasized, "so we are a bit ahead of the game when it comes to complying with HIPAA regulations that take affect in 2005."

Migrating from more than 1,500 domains in Windows NT to less than 150 in Windows 2000 has been a major project for Kindred's IT department over the past four years. It was part of larger effort to consolidate and centralize IT staff and operations that serves nearly 30 departments and 800 facilities across the country.

As part of its consolidation effort, Kindred's IT group built an in-house provisioning application combined with the administrative and security capabilities of NetIQ's Directory and Resource Administrator to address several issues. The goal was to establish a formal access request and approval tracking process, streamline administrative functions across applications and improve accountability for changes. In addition, the move to Windows 2000 AD with the help of Directory and Resource Administrator would reduce the high number of domain administrators and the many IS developers and customer support staff with access to critical production data. Kindred's IT department has been able to reduce its domain administrators by a factor of ten while fully managing the transition to better control of access to user data.

Gains Comprehensive Segregation of Duties with Active Views

"We use a layered security architecture on top of Active Directory whereby access to different tasks in AD is limited according to the appropriate privileges assigned to the user," Ealy explained. "Directory and Resource Administrator allows us to segregate and separate duties to effectively control access and to provide an audit trail of changes in a centralized repository automatically."

Kindred's in-house provisioning system controls the process for requesting and setting up new user accounts and integrates directly with Directory and Resource Administrator. Integrating Directory and Resource Administrator with the in-house provisioning system was accomplished in less than a month, enabling the security team to assign a user account according to its appropriate group and ties user access privileges to specific applications. Only the security team has the ability to add individuals to groups, and control exceptions.

Complete Resource Management Simplifies Windows/AD Administration

Kindred's security team uses Active View Management within Directory and Resource Administrator as a central location for simplifying the administration of user roles. Active Views are sets of user accounts, groups, OU's and other defined resources that define specific job functions and the authority and permissions associated with those job functions. Active Views allows Kindred to distribute responsibility across the company by defining who can do what to whom or to what. The help desk, for example, is able to use Directory and Resource Administrator to perform specific job functions and limited tasks for users.

"With Directory and Resource Administrator we can automatically enforce separation of duties, track requests and approvals, provide auditing capability and minimize excess access by IS personnel that may not be necessary," Ealy pointed out. In addition, Directory and Resource Administrator enables the security team to review and track changes as they occur.

The benefits of Directory and Resource Administrator include highly granular yet automated control of user privileges, the elimination of manual procedures, and timesavings that allow administrative staff to concentrate their efforts on more productive tasks.

Conclusion

"The role-based security management we get with Directory and Resource Administrator allows us to satisfy our internal and external audit requirements for knowing who gets what kind of access to specific information. We use role-based security in conjunction to securing NTFS permissions on files and directories with the role-based groups managed with Directory and Resource Administrator," Ealy said. "This makes it extremely valuable as a compliance tool for showing that we meet HIPAA regulations concerning privacy and security of patient data."

"It would be very difficult to live without NetIQ's Directory and Resource Administrator," she concluded, "since it gives us the ability to ensure separation of duties, automate many manual processes and help us meet new HIPAA regulations all necessary to ensure the appropriate privacy and confidentiality of our patient information."

Contacts

Worldwide Headquarters

NetIQ Corporation
3553 North First Street • San Jose, CA 95134
713.548.1700
713.548.1771 fax
888.323.6768 sales
info@netiq.com
www.netiq.com

NetIQ EMEA
+44 (0) 1784 454500 • info@netiq.com

NetIQ Japan
+81 3 5909 5400 • info-japan@netiq.com
www.netiq.com/japan

NetIQ Australia & New Zealand
61 (0) 2 9959 2313
www.netiq.com/au

For our offices in Latin America and Asia,
please visit our web site at www.netiq.com/contacts