



Healthcare Provider Increases Productivity and Strengthens HIPAA Compliance

Overview

Country: United States

Industry: Healthcare

Customer Profile

Community Health Network (CHN) is an integrated healthcare network that comprises dozens of facilities and employs some 10,000 people. In 2004, CHN posted revenues of \$1.3 billion.

Business Situation

To address challenges in employee productivity and facilitate HIPAA compliance, CHN needed to automate the provisioning of employee accounts and role-based access into clinical systems.

Solution

CHN deployed an identity-management solution based on Microsoft Identity Integration Server and other Microsoft technologies and integrated with the enterprise's human-resources databases.

Benefits

- Employee productivity and satisfaction
- Easier administration
- Proactive approach to provisioning
- Stronger HIPAA compliance



“With these tools, I can know within hours what the current authorizations are for any employee—who has access to what systems and why.”

Dave McClain, Information Systems Security Manager, Community Health Network

Indianapolis-based Community Health Network faces the challenge of providing information technology and services to clinical professionals in a seamless and transparent fashion, while keeping administrative costs down and maintaining stringent compliance with confidentiality laws and practices. To meet this challenge, the organization recently deployed an identity and access management solution based on Microsoft Identity Integration Server and other Windows Server System technologies. With the new solution, the organization is significantly automating user-account provisioning and role-based access control. As a result, new employees can be productive from their first day of work, administrators can focus on more value-added tasks, and the overall enterprise can more easily maintain compliance with HIPAA regulations.



“We liked the flexibility of MIIS that enabled it to comply with the business logic we had in place.”

Dave McClain, Information Systems Security Manager, Community Health Network

Situation

Founded in 1956 and headquartered in Indianapolis, Community Health Network (CHN) is an integrated healthcare network that comprises five tertiary-care hospitals with a total of 1,500 beds, 30 ambulatory care centers, six free-standing surgery centers, three nursing homes, and a primary-care physician network with 120 owned practices.

CHN is known for a focus on primary and secondary care and for its commitment to partnerships—with physicians, with other area healthcare enterprises, and with the community at large. CHN employs 10,000 people and in 2004 posted revenues of \$1.3 billion.

For IT professionals in healthcare, it's not enough to provide fellow-employees with well-designed and smooth-running systems. Those systems also must work transparently, so that doctors, nurses, and other medical professionals will have them when they need them, where they need them, and working in a way that enhances rather than interrupts the care of patients.

For an employee just joining CHN, that could be something as practical as having fully functioning e-mail on the first day of work. For an employee being promoted to a new job, that could be something as critical as ensuring timely access into the clinical systems necessary to get the new job done. For any employee, that could be something as simple as being able to find the current phone number of a colleague who has changed facilities.

Dave McClain is one of those IT professionals who understands the challenges of serving a healthcare community. In his job as Information Systems Security Manager at CHN, he is charged with helping to ensure that systems are available when, where, and

how employees need them—and in a way that also meets other stringent requirements of healthcare information systems such as cost-effectiveness and confidentiality.

McClain started tackling such challenges soon after joining CHN in 2000. Within two years, his group had transformed the process of establishing computer accounts for new employees from one based on paper to one based online. The next challenge for his group was to streamline the process even further.

Delays in Account Generation and Provisioning

As McClain explains, the process of account provisioning for a new employee depended largely on the employee's manager.

“Too often, a manager might wait until a new physician or nurse started work before submitting the new-account request,” McClain says. “It might easily take three or four days before the request was approved and implemented, and by then the individual would have finished orientation and be making his or her rounds on the unit. But without computer access, that individual could not provide the care patients needed without the help of another employee who could access e-mail or the necessary clinical systems.”

When an employee changed jobs, a similar problem occurred in ensuring that his or her account reflected the change. “Even just a few hours' delay in having a working computer account and access into the necessary clinical systems can make it tough to provide the standard of care that is required of a medical professional at CHN,” McClain points out.

“The solution is not only helping new employees to gain access privileges to vital clinical systems more efficiently, it also is helping CHN to remove access privileges from individuals who are leaving employment with CHN.”

Dave McClain, Information Systems Security Manager, Community Health Network

Deprovisioning an Even Bigger Challenge

A bigger problem for McClain and his colleagues was updating accounts when an individual left employment at CHN.

“Although IS security personnel processed termination reports daily, final payroll calculations could leave an employee in an active status beyond his or her last day on the job,” McClain explains. “This was a complex problem for administrators, because most medical professionals at CHN tend to accumulate access into a number of systems over their tenure. And it was a potentially serious problem for the enterprise as a whole, because it meant that the record would show that employees who no longer worked for CHN still had access into sometimes highly confidential clinical systems.”

McClain adds, “The protection of a medical record is paramount when it comes to compliance with HIPAA (Health Insurance Portability and Accountability Act of 1996). So we needed a way to ensure that those access authorizations were fully eliminated.”

Whatever the reason for updating an employee’s computer account and access into clinical systems, McClain notes that the process was inefficient. “Account administrators had to act on every one of the enterprise’s nearly 1,600 requests per month for account creation, modification, or removal, and one person was working full-time just to administering users, user stores, authentication, and privileges,” he says. “We needed a way to automate the process.”

Contact Information Slow to Update

Less pressing, but related, challenges for McClain and his IS colleagues involved the generation of employee phone directories.

“With 10,000 employees in various departments, it was difficult to maintain a

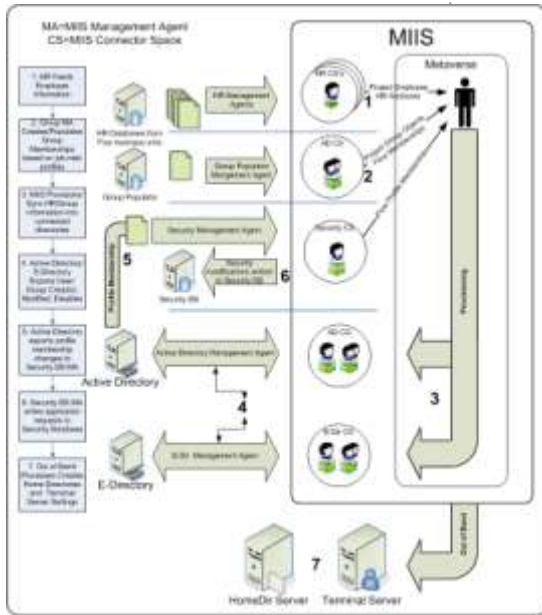
current and comprehensive phone directory for the enterprise,” McClain explains. “An employee who changed jobs was responsible for updating his or her contact information through a process that involved submitting a paper report to a PBX operator. It could take days or weeks or longer, and the phone directory was in disarray, with multiple ongoing complaints.”

Employees also wanted an easier way of managing their account passwords. “There were multiple passwords into various systems, and updating or retrieving a lost password almost always required the help of an administrator,” McClain says. “This was time lost for both the user and the administrator.”

Solution

In early 2002, McClain and his team decided to develop an identity and access management solution that would eliminate the need for much of the human involvement in the process of creating, modifying, or removing employee accounts and access into clinical systems. With a number of Novell technologies installed throughout the enterprise, team members initially selected Novell dirXML for the project. But they soon learned that that the Novell product required extensive customizing to fit into their environment, which was costly and time-consuming from a development standpoint.

So they considered instead an approach based on Microsoft technologies, which also were installed throughout the enterprise, and decided on Microsoft Identity Integration Server (MIIS). “We liked the flexibility of MIIS that enabled it to comply with the business logic we had in place,” McClain says. “We also liked its ability to store and integrate identity information from multiple directories, and its integration with Microsoft Visual Studio.NET for simplifying ongoing development.”



Logical flow of identity information within Community Health Network

Echoing these sentiments is McClain's colleague at local partner MindGent, which played an instrumental role in helping Community Health Network to select MIIS for the project.

"Having worked with Community Health Network since 2001, we set out to apply our experience and expertise in identity-management systems to help our colleagues there select the best technology to help strengthen the hospital's position regarding HIPAA compliance," says Greg Clow, MindGent Identity Consultant. "That technology was MIIS."

Working with Microsoft Consulting Services and Mindgent, McClain's three-person team developed and deployed the initial phase of the solution in a little over a year. According to McClain, individuals from Microsoft Consulting Services (MCS) were central to this effort. "MCS worked hand-in-hand with Mindgent in discovery of information, design and implementation, and ensuring flexibility for future phases," he says.

One of the resources used extensively by Mindgent professionals was the MSSC Guidance references on Microsoft TechNet. According to Clow, "In particular, we used the MIIS Scenario Documentation, MIIS Developer Reference, and the overall MSDN site for reference in coding and installing the MIIS resource kit tool."

The CHN identity and access management solution is based on a number of Microsoft products including Microsoft Identity Integration Server (MIIS) 2003, Microsoft Windows Server 2003, Enterprise Edition, Microsoft SQL Server 2000, Microsoft

Exchange Server 2003, Microsoft Active Directory, and Microsoft ASP.NET.

Within the CHN identity and access management solution, MIIS accesses a number of human-resources databases multiple times daily, to collect attributes from those databases, and to assign a business role to each CHN employee whose name is new or has been updated since the last database access. As a result, whenever someone from human resources enters or updates a employee's name, the employee is provisioned with a new or updated user account and assigned to a new or updated business role based on attributes supplied by the human-resources databases. MIIS stores these roles in a centralized database that acts as the sole authority for identity management at CHN, a database that IS security personnel can access to determine which clinical systems the employee may be granted access to.

A corollary process occurs for updating the employee phone directory. When someone from human resources enters a change in an employee's job or location within a human-resources database, MIIS pulls that information from the database and populates an Outlook address book with it. By centralizing identify information, CHN also allows employees to self-service password management and directory updates.

Benefits

McClain says that the MIIS-based identity and access management solution at CHN provides extensive benefits to management, IS staff, clinical employees, and administration—boosting productivity, helping to maintain and control the appropriate role-based access into clinical systems, and simplifying the account-management lifecycle.

“We set out to apply our experience and expertise in identity-management systems to help our colleagues [at CHN] select the best technology to help strengthen the hospital’s position regarding HIPAA compliance. That technology was MIIS.”

Greg Clow, Identity Consultant, MindGent

Higher Productivity, Job Satisfaction

With the CHN identity and access management solution automating the generation of new employee accounts, hiring managers no longer need to be involved. This approach makes the manager’s job a little easier and helps to ensure that new employees have access to e-mail on their first day of work and access into clinical systems almost always by the time they complete orientation and are working on the unit.

“This helps new physicians and nurses to be productive right from the beginning, which helps to improve patient care and gives the physician or nurse a very favorable first impression of Community Health Network,” McClain points out. “This is essential in healthcare, where it’s always a challenge to find and keep top-notch clinical professionals.”

Yet another advantage of the identity and access management solution for new and current employees is the ability to support an up-to-date phone directory at any time. As McClain explains, the directory is generated at the moment a user requests it. “This helps to ensure it is up-to-date since the last access of the solution to the human-resources database, typically just a couple of hours.” Still another advantage of the solution for employees is a single or reduced sign-on procedure and simplified password management.

Together, these advantages help to raise productivity not only among the clinical employees at CHN but also among managers and administrators. “With automated account provisioning, the individual who used to work full-time processing account updates now is spending most of the day on higher-level tasks, such as comprehensive auditing,” McClain reports. “And with the self-service phone-directory generation and simplified

password management, we’ve reduced the volume of help-desk calls significantly.”

Proactive Process for Supporting HIPAA Requirements

Perhaps the most important advantage of the MIIS-based identity and access management solution at Community Health Network, however, is its support for a proactive, rather than reactive, process for deprovisioning employee accounts.

Referring to one of the central challenges that led CHN to develop the solution, McClain says, “The solution is not only helping new employees to gain access privileges to vital clinical systems more efficiently, it also is helping CHN to remove access privileges from individuals who are leaving employment with CHN. And it is doing this through a consistent account-management process that deprovisions accounts based on standardized queries against identity information.”

McClain explains that this aspect of the solution also gives CHN managers reporting and auditing tools supporting HIPAA requirements on authorization and supervision, workforce clearance, termination procedures, access authorization, access establishment and modification, password management, unique user identification, and person and entity authentication.

“With these tools, I can know within hours what the current authorizations are for any employee—who has access to what systems and why,” McClain says. “We always had access to such information, but never before in such an up-to-date form.”

“Central to our Growth Strategy”

McClain and his colleagues are now working with consultants from Mindgent to implement subsequent phases of the identity and access management solution. In so doing, they are taking advantage of the comparative ease of

“These capabilities are central to our growth strategy as a regional healthcare enterprise.”

Dave McClain, Information Systems Security Manager, Community Health Network

updates made possible by one of the aspects of MIIS that led them to select it as the basis of the identity and access management solution: its integration with Visual Studio .NET.

“When we were starting out, in the Novell dirXML environment, we found it incredibly complex to update the business logic, for example,” McClain points out. “But with MIIS as the foundation of the solution and Visual Studio.NET as our development environment, we can accomplish the same end with just a couple of lines of code.”

Of those new enhancements, two are in process and one is completed. In process are (1) a development that will further automate provisioning so that new clinical employees will have role-based access even sooner than they do now and (2) the incorporation of print-auditing software into the identity and access management solution to streamline internal billing of print jobs.

The recently completed enhancement integrates into the solution a database that supports the credentialing of the 3,000 independent physicians who perform surgeries and other procedures at CHN facilities. The solution provides account provisioning for those physicians in the same rapid and efficient manner it now does for staff physicians. It also manages more than 100 dynamic e-mail distribution lists based on physician specialty for the purpose of enhancing communications and information sharing between the hospital and the physicians.

“With this enhancement, we can demonstrate to the independent physicians how quickly we can meet their access requests and thereby make it easier for them to see patients in our facilities, as well as provide them with focused and timely news and other information pertaining to their respective

specialties,” McClain says. “Along with the other advantages provided by the MIIS-based identity and access management solution, these capabilities are central to our growth strategy as a regional healthcare enterprise.”

For More Information

For more information about Microsoft products and services, call the Microsoft Sales Information Center at (800) 426-9400. In Canada, call the Microsoft Canada Information Centre at (877) 568-2495. Customers who are deaf or hard-of-hearing can reach Microsoft text telephone (TTY/TDD) services at (800) 892-5234 in the United States or (905) 568-9641 in Canada. Outside the 50 United States and Canada, please contact your local Microsoft subsidiary. To access information using the World Wide Web, go to: www.microsoft.com

For more information about Mindgent services, call (888) 464-0331

Or visit: www.mindgent.com

For more information about Community Health Network, call (800) 777-7775 or visit www.ecommunity.com

Microsoft Windows Server System

Microsoft Windows Server System is a line of integrated and manageable server software designed to reduce the complexity and cost of IT. Windows Server System enables you to spend less time and budget on managing your systems so that you can focus your resources on other priorities for you and your business.

For more information about Windows Server System, go to:

www.microsoft.com/windowsserversystem

Software and Services

- Microsoft Windows Server System
 - Microsoft Windows Server 2003 Enterprise Edition
 - Microsoft Identity Integration Server 2003
 - Microsoft SQL Server 2000
 - Microsoft Exchange Server 2003
- Technologies
 - Microsoft Active Directory
 - Microsoft ASP.NET
 - Microsoft Visual Studio.NET

- Microsoft Consulting Services

Partner

- Mindgent LLC

© 2005 Microsoft Corporation. All rights reserved.
This case study is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY.
Microsoft, Windows, the Windows logo, Windows Server, and Windows Server System are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. All other trademarks are property of their respective owners.

Document published September 2005

Microsoft