Security management solutions for the healthcare industry
White paper

Tivoli software

Simplify and help secure access to critical information: Identity management and single sign-on solutions for healthcare providers.

June 2006

ON DEMAND BUSINESS™

Contents

Overview

In the past decade, many healthcare organizations have undergone a transformative shift from paper to digital records. Digitizing patient information has brought about significant benefits: increased operational efficiencies often have lowered costs, while faster access to comprehensive patient information has helped clinical staff make accurate, informed decisions. In turn, the potential to provide higher quality care through on demand access to information has helped reduce the ever-present threat of litigation.

Recently, however, an emerging shortage of healthcare workers has left healthcare organizations in a quandary. On the one hand, they must rely on a constant stream of temporary workers and visiting clinicians to supplement their permanent staff. But on the other hand, connecting temporary workers to the systems and applications that house critical patient data can open healthcare facilities to considerable security risks and management costs.

Adding to these challenges is the increasing demand for privacy and transparency. These requirements are forcing those in the healthcare industry to examine their data management closely, especially in relation to access rights, information sharing and audit trails. The challenge is to provide access in a way that enables organizations to comply with regulations and privacy requirements and that does not place a burden on IT staff or hospital staff – who cannot afford to lose time they could spend on patients.

Highlights

Enforce compliance with access and identity policies across the enterprise

An automated and centralized security management solution can help healthcare organizations enforce access and identity policies consistently across their enterprises. In doing so, they can more easily manage the growing number of users who come in contact with IT systems and reduce the costs of responding to audit requirements.

This white paper discusses the advantages of IBM security management offerings, which are designed to deliver integrated, end-to-end identity and access management solutions across a heterogeneous environment. Specifically, this white paper discusses how this comprehensive offering of software, services and expertise from IBM can help healthcare organizations create an on demand environment in which clinical staff can access the information they need quickly – and securely.

The challenge: Protect confidential information without adding complexity

In the vastly more mobile world of today's healthcare organizations, physicians often work with many hospitals, while traveling nursing staff regularly rotate from unit to unit and facility to facility. To accommodate these users, many healthcare organizations have implemented kiosk and shared-workstation environments to support larger numbers of users per workstation. While these cost-effective measures provide fast access to patient data, they can also expose sensitive data to a serious security risk.

Passwords – implemented to protect these and other systems – can quickly become a burden for IT staff and clinical staff alike. Often, employees must log on and off a dozen or more times an hour to access data from multiple password-secured systems. At any given time, hospital staff may maintain

Highlights

anywhere from 5 to 15 passwords – some of which must be changed as often as once every 30 days. And if they forget one of their many passwords, healthcare staff have few or no options other than to wait for the help desk to reset the password – time that staff could be spending on patients. Furthermore, many solutions require clinical staff that use kiosks to log on to Microsoft® Windows®, and – as a result – force users to wait while Windows boots before they can access patient records. Ultimately, the time lost to these password-related inefficiencies can represent millions of dollars per year in lost productivity.

Simplify system access procedures to help maintain security while aiding productivity

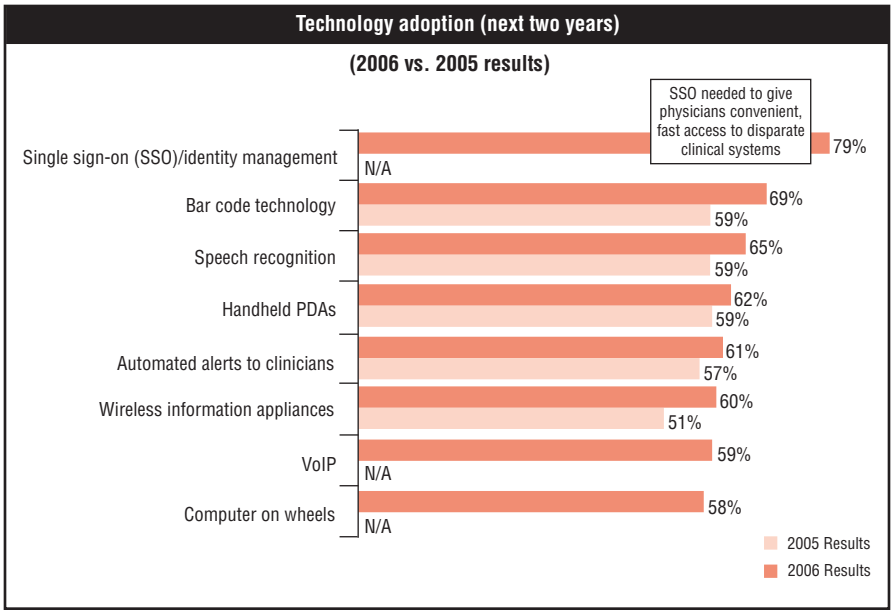
These productivity losses are not just limited to hospital staff. In addition to the time spent on routine tasks such as resetting passwords and updating accounts, IT staff are taxed with the pressures of granting new staff members access to the systems that house critical patient data – and removing access immediately when an employee leaves. Preventing unauthorized access to critical patient systems, however, is made that much more challenging when employees can change from month to month. Every time someone changes jobs, roles or employment status, their user access must be appropriately adjusted by altering or deleting all of their user accounts across every application or system. The processes and procedures used to grant access rights to users must also be tracked to ensure audit compliance. To achieve audit compliance, teams of IT staff must perpetually audit each production server and application manually to avoid invalid accounts and the potential for inappropriate access.

Identity and access management solutions can help reduce the burden on everyone across an organization – from IT staff to visiting physicians

to supplemental nursing staff. The solutions provide critical capabilities, including the following:

- Maintaining access rights and privacy preferences based on preset policies.
- Provisioning and deprovisioning users quickly.
- Streamlining password management.
- Helping reduce the time and cost of addressing regulatory privacy mandates.
- Empowering users to perform simple password resets.

These capabilities enable a healthcare facility to regulate access to critical applications in compliance with security processes, while providing a responsive, efficient environment for clinical staff.



Among their technology priorities for the next two years, healthcare CIOs identify single sign-on and identity management as the top priority. Source: 2006 Healthcare Information and Management Systems Society (HIMSS) Leadership Survey.

Highlights

Efficiently manage access for different types of users to help comply with policies and regulations

Manage user accounts across the enterprise

Establishing a single point to manage user identities is the first step toward bringing structure to rapidly changing user populations. A centralized identity management solution can help IT provision and deprovision users from a single location. By administering access in a uniform manner, the organization can gain visibility across the enterprise into exactly who has what rights. This visibility lets IT track everyone who has access to systems and assign access based on the organization's access policies and on the user's role. As an example, a chief of staff for a large hospital requires a different set of privileges than a remote worker processing health claims for an insurance company.

The policies the organization establishes automatically apply rules that govern the type of access given to each group of users – such as temporary staff or administrators. They also establish a baseline against which the organization can perform meaningful auditing and easily identify noncompliant events. When users no longer require access to a particular set of resources, IT can immediately suspend or delete the appropriate accounts to help ensure that sensitive data remains confidential.

Identity management solutions also help organizations maintain accurate records of access rights changes for auditing purposes – helping reduce the cost in terms of staff time and money needed to comply with audit requirements.

Case study: Duke Medicine
With more than 2,000 staff members and a constant stream of visiting physicians, Duke Medicine — one of the top 10 healthcare institutions in the United States — needed a solution that would support fast, secure access to medical records and diagnostic systems without compromising patient confidentiality. Ideally, the solution would enable IT staff to provision and deprovision users quickly, and provide self-service capabilities that would empower healthcare staff to manage simple password resets and routine tasks on their own.

After implementing IBM Tivoli identity management software, Duke Medicine was able to automate and streamline the user provisioning and deprovisioning process while enabling users to efficiently and securely access vital patient information. When new and visiting clinicians need to access the hospital's online systems, order medications or request lab tests, they can quickly log on to the applications they need. And with fewer passwords to remember and the ability to perform simple IT tasks themselves, clinical staff have more time to spend caring for their patients, while IT staff have more time to focus on higher value activities.

An integrated identity management solution can help healthcare organizations:

- Reduce costs associated with managing identities by automating processes and reducing technical support needs.
- Centralize identity life-cycle administration.
- Increase efficiency of access control processes and obtain constant visibility into who has access to what.
- Improve productivity and usability for users and administrators through self-service capabilities for account updates.
- Facilitate audit compliance with greater ease and less cost.

Streamline authentication management

Password-related complexity is one of the greatest sources of lost productivity for healthcare organizations. The time spent entering and resetting passwords is lost in small, infrequent increments – which add up to a significant consumption of time spent away from patients. Even more importantly, poor password selection and management by employees represents one of the biggest security weaknesses in IT today. For example, many workers log in to kiosks and walk away without logging off.

A unified authentication and enterprise single sign-on solution can help maximize security, convenience and productivity. Single sign-on is a simple way to tie together proper user authentication and application access while enabling stringent privacy controls. Single sign-on accelerates access, eliminates the need for health practitioners to remember multiple passwords and helps retain a high level of security for each application. When combined with context management capabilities that aggregate all relevant patient information across disparate applications, single sign-on enables staff to

Highlights

gain a comprehensive view of a patient's healthcare life cycle. For example, a doctor can access all records of past visits, prescription information and other medical data that resides in separate applications through a one-time authentication process.

Authentication capabilities address a number of scenarios – from desktop password resets and shared-workstation spaces to support for multiauthentication requests that include smart cards, biometrics and tokens.

Help reduce losses in time and productivity by offering simple, secure, self-serve access

A unified authentication and single sign-on solution can help healthcare organizations:

- Provide convenient, proximity-based authentication.
- Improve clinical user productivity through self-service password resets.
- Secure access across clinical shared workstations.
- Improve patient safety and reduce clinical errors.
- Ease the costs of compliance.

Start with IBM Tivoli security management solutions

Solutions from IBM Tivoli® software can help healthcare organizations address the specific challenges their facilities face. Single sign-on access, centralized user account creation, policy-based control of access rights and self-service interfaces help reduce administration costs and help control access to sensitive information, while managing it to facilitate compliance with audit requirements.

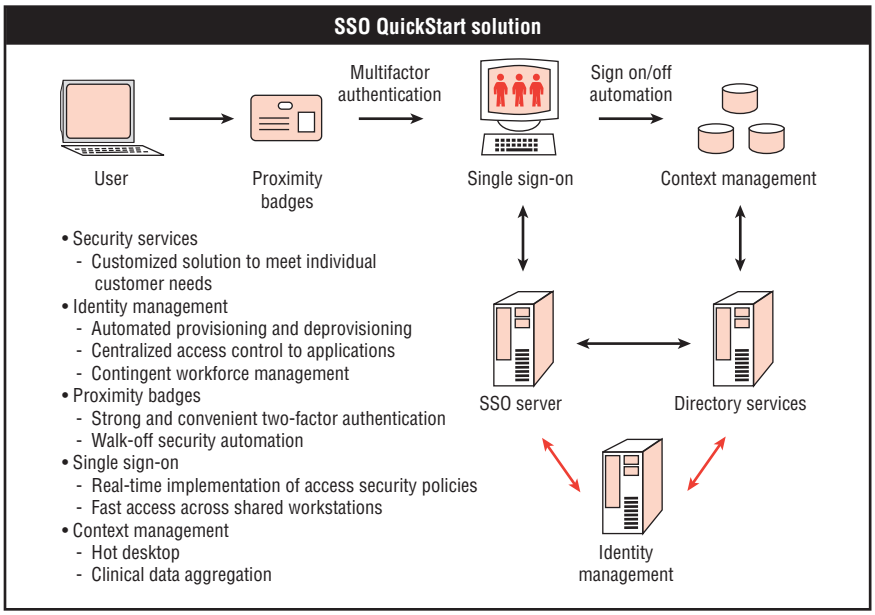
The comprehensive suite of specially designed security management software includes:

- *IBM Tivoli Identity Manager,* which automates the business processes of provisioning and deprovisioning users across the infrastructure, in compliance with the organization's security policy. The software features a standard recertification and reconciliation process to confirm all accounts are active and valid. Additionally, Tivoli Identity Manager adapters offer "out of the box" support for many of the most common applications in the healthcare segment.
- *IBM Tivoli Access Manager for Enterprise Single Sign-On software,* powered by Passlogix®, which streamlines the processes for authenticating a healthcare professional's access to multiple applications, including clinical applications. At the same time, it helps protect data confidentiality and integrity. Tivoli Access Manager for Enterprise Single Sign-On adapters extend base functionality to support shared workstations, desktop password resets, automated credential provisioning and multiauthentication methods. Tivoli Access Manager Enterprise Single Sign-On software supports multiple off-the-shelf and customized clinical applications from McKesson, Meditech, Cerner, Siemens, Epic and GE.
- *IBM Tivoli Access Manager for e-business,* which offers a policy-based approach for clearly controlling who can access what, and a comprehensive auditing infrastructure to help demonstrate compliance with access rules and simplify audit activities.
- *IBM Tivoli Security Operations Manager,* which centralizes and stores security data from throughout the IT infrastructure to automate log aggregation, correlation and analysis; enforce security policies; and provide comprehensive reporting. By automating the process of detecting breaches of confidential information, healthcare organizations with limited security resources help protect the confidentiality of data and facilitate efforts to comply with audit requirements.

Leverage IBM expertise and experience

Tivoli software for the healthcare industry is backed by world-class IBM services, an extensive ecosystem of partners and focused research. IBM Tivoli security management solutions are designed to interoperate with other IBM infrastructure management solutions to help support additional requirements, including context management technology from IBM WebSphere® Portal and Carefx.

To help organizations get started quickly, IBM Software Services for Tivoli offers QuickStart services that enable rapid installation and implementation of Tivoli Access Manager for Enterprise Single Sign-On, Tivoli Access Manager for e-business and Tivoli Identity Manager. IBM Software Services for Tivoli leverage best practices gained through hundreds of implementations to help prevent security complexity and protect private user information in accordance with regulatory compliance efforts.



IBM QuickStart Services for Tivoli Access Manager for Enterprise Single Sign-On help healthcare organizations combine identity management, proximity badges, single sign-on and context management capabilities into a solution that is customized to fit an organization's particular needs.

Summary

With an increase in mobility across the healthcare organization today, staff members fluctuate frequently from month to month. Healthcare organizations must find a way to give these users the access they require without compromising patient data integrity or complicating their ability to meet regulations.

Establishing a central point to manage user identities and access can help an organization securely manage the growing number of users who come in contact with IT systems and give users the tools they need to be more productive – and to provide higher quality care. Simplified end-user access enables users to get the information they need quickly and without the frustrations of logging in and out of every application they access multiple times each day.

Beyond protecting assets, these capabilities can help facilitate and reduce the compliance costs while reducing administration costs. The end result? The potential to provide better clinical care at a lower overall cost-revenue ratio.

About Tivoli software from IBM

Tivoli software from IBM helps organizations efficiently and effectively manage information technology (IT) resources, tasks and processes in order to meet ever-shifting business requirements and deliver flexible and responsive IT service management, while helping to reduce costs. The Tivoli portfolio spans software for security, compliance, storage, performance, availability, configuration, operations and IT lifecycle management, and is backed by world-class IBM services, support and research.

For more information

To learn more about how IBM can help your healthcare facility drive the reliability and service quality of your critical applications, contact your IBM representative or IBM Business Partner, or visit **ibm.com**/tivoli

IBM Corporation
Software Group
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
6-06

GC28-8435-00