

Issue Date: Online

Not too Tight, Not too Loose

Today's healthcare environments require an enterprise approach to identity management that ensures security while letting clinicians practice.

by Mychelle Mowry and Reid Oakes



In healthcare, the swift digitalization of clinical and financial data offers promising benefits, including reduced costs, higher quality of patient care, and a channel to include and help educate consumers. The growth of electronic data in healthcare, however, has been accomplished through a relatively non-structured approach to IT procurement, leaving provider organizations to support numerous clinical and administrative systems while lacking a single-support and security framework to effectively manage the high volume of digital data. The resulting situation is a maintenance nightmare with increased risk of access and security breaches.

A recent study of more than 850 provider organizations by the board of the eHealth Vulnerability Reporting Program revealed that the security of electronic health records (EHR) is squarely at risk. Indeed, some industry experts estimate that as many as 77 people could view a patient's record during a typical hospital stay. While necessary to ensure access for clinicians focused on saving lives, it is equally important to protect the security and privacy of sensitive patient data from inappropriate use.

To reduce risk, streamline IT management and enhance compliance, progressive healthcare organizations are rethinking their approach to identity management — moving toward an automated enterprise-wide framework that treats identity management as a centralized IT service, as opposed to an embedded, duplicate functionality in every application deployed. This approach enables organizations to effectively manage access, role management and the end-to-end lifecycle of user identities across all enterprise resources.

Protected Health Information (PHI) spread across numerous clinical and enterprise systems challenges an organization's ability to secure, audit and report on data access. Maintaining critical data points in multiple systems with separate security roles and asynchronous privileges increases the potential for error. As organizations look to implement longitudinal patient views or collaborate with other providers, the complexity associated with best-of-breed solutions greatly increases the cost of success.

By deploying an automated identity framework, organizations can consolidate practitioner access roles and privileges, ensuring practitioners have access to *all* relevant data in the enterprise. The automated framework also enables centralized reporting and policy enforcement, decreasing the time and cost associated with Health Insurance Portability and Accountability Act (HIPAA),

Sarbanes-Oxley (SOX), Joint Commission on Accreditation of Healthcare Organizations (JCAHO) and other privacy and security compliance requirements.

Simplifying the provider experience

Healthcare organizations are challenged with managing two opposing requirements — the practitioner’s need for easy access to information versus the organization’s need to apply increased privacy and security controls against that data. Excessive security within a healthcare organization limits its ability to provide effective and efficient patient care. Conversely, the lack of sufficient security makes the organization vulnerable to legal and civil penalties. **Clinicians need solutions that minimize the number of keystrokes required to access information; however, best-of-breed IT strategies have complicated this process.**

Physicians spend on average seven minutes per patient encounter, of which they spend nearly two minutes on managing logins and application navigation. Likewise, an average major healthcare provider has more than 150 applications — most requiring different user names and passwords — making it difficult for caregivers to navigate and receive contextual information. Healthcare organizations must strike the right balance, in terms of simplifying access to core clinical data sets while maximizing the time providers can interact with patients without jeopardizing data integrity and security.

To simplify the provider experience, organizations need to bring multi-faceted identity-based services to the end-user level. Many organizations have undertaken “phase1” project initiatives, such as enterprise single sign-on, contextual management or adaptive authentication. While a good start, these initiatives alone do not provide a comprehensive solution. To fully address the problem, healthcare organizations require an enterprise approach that encompasses enterprise single sign-on, context management and adaptive authentication — as well as the ability to deliver fast and efficient enterprise-wide workflow to manage the user experience.

➤ Single sign-on and context management

An enterprise single sign-on service must integrate not only with clinical systems, but also with critical network and infrastructure components such as e-mail, file sharing and enterprise collaboration services. While enterprise single sign-on improves the user experience when accessing multiple applications, it only provides the initial authentication to the system. To mitigate risks, providers must also provide context management.

The promise of context management is often limited by an organization’s ability to upgrade to context-management-compliant versions of its critical applications. Because most organizations cannot wholesale upgrade applications across the enterprise in support of a context management initiative, a better approach is to integrate applications through single sign-on and provide context management when the provider accesses a system that supports it. The initial benefit the provider experiences through single sign-on and password management will allow the IT department the opportunity to investigate integrating non-context management compliant applications.

➤ Adaptive authentication

Adaptive authentication analyzes access risk and requests different levels of information from users depending on the level of risk. For example, clinicians working in a low-risk environment (such as an IT resource located on site) may be granted access to information with a simple user name and password scheme. In situations that present more risk (such as when a user is logging on from a remote location or from a PC that is not owned by the provider), the system may require users to provide more detailed information upon sign in, which may include their last day off work or the last facility in which they provided care. Adaptive authentication allows organizations to ensure a simplified provider experience while providing higher access thresholds based on perceived risk.

➤ Advanced workflow support

Simple technology-only identity management solutions force changes to the way providers manage their patient flows or clinical presence. In order to gain the most benefit from the technology, however, an identity management framework solution needs to be flexible

enough to drive simplification without dramatically changing or re-architecting user expectations or workflows.

Enterprise role management

Healthcare organizations utilize numerous staffing methods, including contract nursing, physicians, specialist groups and students. Organizations must maintain staff privileges and levels of authority in a system of record for contract employees, students and permanent staff. Granting appropriate access to enterprise systems and applications is often a time consuming process that leads to significant "down time" in which the user is on site but not yet provisioned appropriately. Further, it requires resources in IT to manage all the changes. An additional challenge of provisioning is the possibility of granting incorrect permissions to an individual. If an error occurs due to manual mis-provisioning, the organization is often unaware until an audit reveals the infraction.

When a new user joins a department, the hiring manager typically requests access to IT systems through help-desk work orders, e-mail requests or phone calls. The manager may request that IT grant the new employee the same privileges as another team member who performs a similar role. This method breaks down, however, as organizations transfer and promote people within the organization. Organizations that perform attestation (reviewing each user's appropriate versus configured privilege) less often are at greater risk for inappropriately authorized access.

Advanced role management capabilities are allowing healthcare providers to address both the issues of manual mis-provisioning and inappropriately aggregated privilege. As users change roles or user roles change, the system can append or deprecate individual privileges automatically to reflect the new responsibilities. Because the provisioning process is workflow driven, approval and denial of access is logged for audit. When users leave the organization or their access is no longer required, the organization can revoke user access through a one button de-provisioning process.

Advanced role management systems also assist in the development of roles by uncovering roles currently utilized in enterprise and clinical systems and aggregating the policies used to govern these roles. These systems use sophisticated statistical analysis to determine user and privilege relationships and then cluster these relationships into candidate roles.

Streamlined compliance reporting

Regulatory compliance and mitigating the risks associated with insider threats are two of the most complex and costly security challenges healthcare providers face today. To meet these requirements, providers not only have to protect sensitive information, they also need to monitor access. **The cost and complexity of enterprise wide certification can be astounding and the diverse audit services within enterprise and clinical systems make it very difficult to develop a consistent end-to-end audit trail for end-user activity.** New solutions are enabling providers to collect and consolidate audit data transparently, providing valuable insight into who did what to which data and when, including privileged users who have direct access to the database.

Managing the practitioner's need for ease of access to information versus the business's need to apply increased privacy and security controls against that data is becoming more difficult as organizations implement new systems, capabilities and products to serve their constituents. Provider organizations that move toward an enterprise approach to identity management are well positioned to strike the right balance between provider enablement and data security requirements today and into the future.