



Effective Identity & Access Management Solutions Take Healthcare to the Next Level

Andrew J. Hurd

Andrew Hurd is the Chairman and CEO of Carefx based in Scottsdale, AZ.

As healthcare organizations, including hospitals, Regions, and LHINS open their networks to more employees, they must deal with the challenge of providing accounts to multiple users, each with the appropriate level of access to applications and resources; often times to applications the users may not be familiar with. They must also simultaneously address all aspects of user administration, authentication and access control.

It is not uncommon for large healthcare organizations to run dozens of different applications developed and supported by just as many vendors. Even in the case of a “single vendor HIS,” there are myriad departmental solutions that add to the complexity. Increasingly, these hospitals want to integrate the flow of information between applications internally, and to link their systems with partners, suppliers and regional health information organizations (e.g. Regions, LHINS, and Provincially). The problem is that, in most cases, the applications aren’t integrated. Each has unique logon procedures and patient-selection processes, making information access difficult, time-consuming and frustrating.

Industry analysts Frost & Sullivan define identity and access management (IAM) as “the process of managing authentication, access rights, privileges and administration of digital users.” The ideal Identity & Access Management (IAM) solution should be open, flexible, and scaleable — meaning that it interoperates with the existing IT infrastructure (even if there are several behind the scenes), including applications, operating system, and hardware. A closed, proprietary system can result in unnecessary costs, lost ROI on existing investments, and prolonged deployment schedules.

IAM also addresses care providers’ need to access patient information stored in multiple applications quickly, intuitively and remotely, and allow for secure, time-saving, user-friendly access to a patient’s entire medical record, enhancing providers’ ability to deliver

quality care. In essence, IAM mitigates the user’s need to know specific applications to get to the relevant data they need, speeding the care-delivery process.

While simplified access to applications is helpful, the big payoff for clinicians comes with the robust and intuitive workflow at the patient, result and object level that is delivered through context sharing, or context management. Context Management offered as a component of an IAM solution provides for the type of real-world interoperability that will quickly and efficiently deliver meaningful clinical workflow in a way that clinicians need and have always envisioned. This represents a quantum leap forward for healthcare organization, where, traditionally, finding all relevant patient information for the most accurate diagnosis and treatment required clinicians to access and search multiple applications — an unnecessary and time-consuming process. This challenge has been compounded by the formation of Regions and LHIN’s, as well as Infoway’s vision for an iEHR.

Navigating the Patient-Information Maze

For HCOs that have invested in large, integrated clinical information systems, such as those from Meditech, Cerner, Siemens or GE Healthcare and best-of-breed implementations at the macro-level, frustrations still exist at the end-user level. These hospitals should seriously consider only those vendor solutions that:

- Interoperate with their existing systems
- Streamline hospital workflow.
- Maximize operational efficiency, improve clinician satisfaction, and provide capabilities beyond single sign-on (SSO).

End-users, including both clinical and business office users, must be able to sign on once to access various systems, drill down into the application and look at patient tests, lab results, diagnoses and other data — all in a role-based view.

With the use of multiple information systems within hospitals and a number of healthcare organizations taking a “best-of-breed” approach, end users are burdened with the need to manage and use multiple passwords and IDs, as well as recall the navigational nuances of each application. In large healthcare systems where physicians may support multiple hospitals, the burden is multiplied, because each hospital may require a different set of credentials to log onto the network and clinical systems, and then find themselves confronted with a dizzying array of user interfaces and application-specific workflows.

This situation has forced many clinicians to navigate the system by sharing IDs and passwords or using generic group IDs to bypass tedious logon protocols. The issue with the latter is that this violates privacy regulations, which stipulate that users must have a “unique identifier” when authenticating to systems that store protected health information (PHI) or patient data.

Compounding the problem: Physicians and nurses spend significant time and effort gathering and organizing patient information to make informed clinical decisions and deliver the best care. In fact, on average, physicians, nurses and staff interface with anywhere from five to 12 different applications as they diagnose patients and devise treatment plans. In addition, they may also spend up to a third of their day jumping between applications looking for lab results, clinical documentation, medication orders and the like; this is after they have logged in to those applications. This is time they could be using to treat sick patients.

The best technology adds measurable value to the clinical realm by functioning correctly and efficiently while minimizing implementation costs. It lets medical personnel define the context of use as they switch between various information management systems. More importantly, in selecting among possible clinical systems, hospitals will want to minimize medical errors and reduce costs. For instance, how much time and money could hospitals and the government save by not ordering duplicate tests?

Turning Theory into Practice

Consider how IAM technology can work in a given hospital (let us call this one “Provincial Health General”). A nurse logs into an application and selects a patient, encounter or observation. The system automatically finds and links related patient information in all other applications. As the nurse toggles from one application to another, the system follows that specific patient — no more repeatedly entering patient IDs or searching lists of patient names. In fact, the human-error factor is greatly reduced while the user’s productivity is heightened.

In addition, by linking all clinical applications at the user-interface level, information entered into PHG’s system is automatically accessible across applications

and instantly available to nurses, physicians and the lab. No one has to wait for lab results or charts to be passed around or make their way from the lab to the treating clinicians. In Provincial’s emergency department, efficient workflow and quality care depend on providers’ ability to quickly access patient information stored in multiple applications. In response, IAM can greatly improve providers’ ability to find accurate information and respond in a timely manner.

Furthermore, because it selected an open IAM platform, instead of a closed, propriety one, Provincial had no need to replace existing systems, the platform links the hospital’s legacy applications that nurses, physicians and support staff are already comfortable using. As a result, there is no steep learning curve, as one might expect when a new system is deployed. Furthermore, the IAM solution can be used to link Provincial and National solutions, such as those being deployed as part of the iEHR initiatives of Canada Health Infoway and other organizations.

Hospitals like our hypothetical Provincial Health General reap tangible benefits in short order. Physicians and nurses can enter orders for a full series of labs for an ER patient and get results back in less time than it used to take just to initiate an order. That efficiency is made possible by linking applications, providing simplified access to patient data and making the new system easy to learn and use. Hospitals can then ensure that providers have expedient access to all the information they need to help diagnose and treat patients.

Remembering multiple IDs and passwords to access multiple applications, waiting for lab results and medication orders to make their way back to the bedside, holding out for data to be entered into the system — can all become a thing of the past. Removing time and workflow obstacles not only helps makes everyone’s job easier, but also, and more importantly, improves clinical efficacy and reduces human medical errors.

Preparing the Organization for IAM

IAM solution benefits far outweigh the costs. If you are in a position to “sell” an IAM solution to others in your organization, be prepared to explain what it can improve. One challenge is to get people to understand what you’re trying to do. Administrators and executives who have secured financing for IAM projects say the secret is to avoid being bogged down by discussing the technical details of Single-Sign-On or Context Management and other elements of security infrastructure. Instead, they present the business case:

The SSO aspects of IAM reduces IT administration and help-desk costs (by reducing the manual hassles of resetting passwords and assigning application access), and Security improvements (no more passwords on scratch paper under the keyboard). But the integrated capabilities of Context Management with SSO can

enhance user productivity (because personnel needn't repeatedly log onto and navigate multiple systems) by as much as 3-times what SSO alone can deliver.

Commonly, the business-process issues present bigger hurdles than the technology itself. Personnel inside the hospital who will manage the project should walk through processes and rules related to identity creation and resource access, such as: Who is able to create, modify and view employee IDs? And what is the trigger for giving a new employee (or an employee changing jobs) access to systems—and for revoking access when an employee leaves or changes roles?

Technology analysts from Gartner recommend that enterprises implementing IAM solutions:

- Obtain cross-organizational buy-in and form a cross-organizational project team. IAM implementations can result in enterprise-wide changes in business processes, which may, in turn, raise political issues that can derail the implementation. Ensuring cross-organizational buy-in early in the project can mitigate this risk.
- Obtain executive sponsorship. Enterprise-wide IAM solutions can be expensive, but they also can result in significant savings to the enterprise. Return on investment will be increased by the inclusion of as many business units as possible.
- Don't expect to find one authoritative source for user data. A more desirable and achievable goal is to have one authoritative repository for user access information that can be used in managing a secure access control infrastructure.
- Implement the IAM solution via a phased project approach. A sound understanding of the enterprise's strategy for Web-based applications, directory services and portal use will help IT decision-makers prioritize the implementation of the various solution components, such as user provisioning, extranet access management, password management and single sign-on, according to their importance to the enterprise. The time and resources required to integrate custom applications should also be analyzed because they can dramatically increase the professional service fees associated with the implementation.

Triple-Digit ROI

A wide range of factors — including the demands of enterprise resource planning implementation, regulatory compliance issues and the pressure to contain costs — are pushing the healthcare industry to better manage IAM issues. IAM solutions, which can offer three-year return on investment (ROI) in the triple-digit-percent range, are becoming essential tools to effectively manage not only user account and access-rights to information across heterogeneous IT environments, but also the entire user experience.

Tracking the locations where user credential and authorization information is stored has become a major management challenge. But, armed with the right technology, hospitals can achieve unprecedented efficiencies through reductions in application development, security administration and help-desk staffing.

What's more, investing in secure electronic patient data aggregation tools that clinicians like and will use must be a high priority; without tools to efficiently provide consolidated views of clinical information, investment in all other initiatives will yield less than anticipated benefits. ●

IAM in Brief

Three main information aggregation tools are used by hospitals that streamline sign-on procedures, simplify access to real-time patient data and ensure security, patient privacy and compliance with regulations.

- Single Sign-On (SSO) — allows clinicians to sign-in to all relevant and authorized applications with a single user name and password.
- Context Management — provides a means for non-integrated, non-interoperable applications (such as disparate legacy clinical systems) to link information at the user interface level so they appear to act like a single system. In so doing, the applications operate in a context-aware environment, allowing users to access and review all relevant patient data in a unified view regardless of where the data is actually stored.
- Compliance Management — automatically tracks each occurrence of patient information access for security, privacy and regulatory compliance purposes.

Collectively, the components of an IAM platform provide simplified, real-time and integrated access to a selected patient's clinical information across all applications, wherever it may reside, and deliver a paper trail to ensure regulatory compliance.

Carefx Corp., based in Scottsdale, Arizona, has more than 200 hospital clients in the U.S., Canada and Europe, and works with global technology corporations such as GE Healthcare, Cerner, IBM, Citrix, McKesson and Siemens.