White Paper

Patient Identity Management: A Dose of Patient-friendly Security for Medical Providers

Robust identity verification and authentication strategies help safeguard meaningful EMR users — and achieve meaningful benefits — of digitally driven care.

LexisNexis®

Risk Solutions

A diet of "everything online:" Good for health care...but hard to swallow?

Every day, in hospitals and physician offices everywhere, health care providers are telling patients what's good for them: Exercise. Eat better. Quit smoking. No one would deny this is great advice — but getting the patient to follow it can be a challenge for reasons most of us know too well.

Ironically, some of these same providers find themselves playing the role of resistant patient in the evolution of digital health care. Tools such as online patient portals and telemedicine offer fantastic opportunities for improving access to care and improving patient satisfaction levels while reducing delivery costs. Yet, as the federal government institutes a phased-compliance approach toward a fully digital health care delivery system — complete with patient portals, electronic medical records (EMRs) and multi-provider data exchange — evidence reveals that some providers may still not recognize the benefits of digitization and related remote access technologies.

However, research shows that a well-outfitted portal offering online patient registration, appointment scheduling, prescription refills, lab results and provider consultation will ultimately:

- **Reduce the costs** of care delivery and administration;
- **Improve patient participation** in their own care, and subsequently improve adherence to therapies and physician guidance; and
- **Increase access to care,** possibly leading to faster intervention and faster decision-making by the care team.

In a recent interview with American Medical News, Dr. Adam Darkins, chief consultant for the Department of Veterans Affairs Office of Telehealth Services, cited remote monitoring as key to reducing days in the hospital by up to 30% and increasing patient satisfaction by up to 70%.

Patients seem enthused about gaining more control over their health care through self-service online and telephony features. In Deloitte's 2011 Survey of Health Care Consumers in the United States:

- **66% of patients said they would consider switching** to a physician who offers access to medical records through a secure Internet connection;
- **52% indicated they would use a smart phone or PDA** to monitor their health if they were able to access their medical records and download information about their medical condition and treatments; and
- **61% express interest in using a medical device** that would enable them to check their condition and send the related information to their doctor through a computer or cell phone.

Reported cost savings from online portals:

- 63 cents for every lab result delivered online (HealthPartners integrated health system and health plan)
- $7 for every appointment scheduled online (Northshore University Health System)
- $17 for every billing inquiry handled online vs. of by phone (Northshore)
- 25% fewer post-surgery follow up visits required (Geisinger Health System)
- 12,000 less phone calls a month (Geisinger)

So what's the problem?

Despite the many potential benefits of EMRs and patient portals...the federal government's adoption incentives... and patient interest in remote access to services, some patients and providers worry about the risk and privacy implications of more widespread patient access. It's easy to understand why:

- Though the majority of consumers in the Deloitte study said they want to use online services, 39 percent of them say they are concerned about the privacy and security of the information shared over Internet-based technologies.

- Anecdotally, providers worry about the potential liability of information getting into the wrong hands through fraudulent access.

- Identity theft has evolved beyond stolen wallets; enterprising fraudsters are now able to steal user credentials in a number of ways. They remotely and surreptitiously download software onto users' systems; capture personal data off of stolen mobile phones; and piece together login and password combinations from personal data offered up in social media. (Birthdates, favorite teams and pet's names don't make for strong passwords.)

At the heart of the issue is a desire to ensure that those who access protected health information are indeed who they claim to be. The identity management industry calls this authentication. Patients and anyone on the care team, including physicians, nurses, and office staff who requires access to this highly regulated data, need to be authenticated prior to being granted access to act as a layer of defense against those who would otherwise use the information for misdeeds or fraudulent activities.

Applying identity management in health care

Identity management services that can remotely authenticate a unique individual and faster more self-service features are a crucial first step in achieving higher utilization levels of service offerings such as patient portals and telemedicine while still protecting sensitive patient information and limiting risk for the provider organization.

This is an environment where information is highly sensitive, providers are time crunched, and decisions often need to be made quickly. Accordingly, an identity management solution needs to be comprehensive yet flexible so as not to hinder the delivery of efficient, high quality care. Best practice calls for a two-phased approach of identity verification and authentication.

Step One: Who are you (and can you prove it?)

When patients enroll for an online portal, call a nurse hotline, or use a mobile application to communicate with the care team, they can be taken through an identity verification and authentication process to 1) collect demographic data, 2) validate that the presented data is correct and up-to-date, and 3) validate that the person presenting the data also owns the identity information being presented. A range of demographic information may be solicited from the user: name, address, date of birth, gender, phone numbers and even a full or partial social security number. The information presented can be compared to trusted data sources to confirm the identity is legitimate, and authentication services like dynamic knowledge-based authentication (dynamic KBA) can assure that the identity does in fact belong to the individual requesting access.

A dynamic KBA engine utilizes trusted data sources like public records to generate multiple-choice questions for which only the patient would know the answer. In order to help thwart would-be imposters, the questions include information not commonly found in a purse, wallet, social media sites, utility bills, or internet searches. This approach works well for remote patient access because 1) the multiple-choice question set is designed based on the sensitivity of the data or services being accessed and 2) different multiple-choice questions are generated each time the enrollment is attempted.

An intuitive, self-registration process used in patient portal or mobile application scenarios—or an equivalent process completed in a call center environment—helps patients gain the desired access in a highly secure way without leaving the comfort of their own home. It's during the enrollment process that the methods for subsequent secure access can be defined.

Step Two: Authenticating the identity during subsequent sessions

Granting initial access to remote patients or providers is one thing, but facilitating simple and user friendly repeat access management and password resets is wholly another.

A best-practice approach goes beyond a simple username and password to utilize two or more aspects of the enrolled user's identity to validate the requestor's identity. Access management is where multi-factor authentication (MFA) comes in to ensure that the person who is requesting access is indeed the enrolled user.

Identity management in practice

Scenarios

Patient portals that don't test patience. To offer more self-service options to their patients and minimize time spent with routine requests, one health care company used multi-factor authentication to make it easier for patients to request prescription refills online.

Using a combination of something they have (filled prescription Rx) and something they know (dynamic KBA), the organization was able to offer faster, less manual access to prescription refills. Of those who were offered the quiz to complete their refill request, 90% passed, 5% failed and only 5% opted out.

Meeting Meaningful Use standards with excellent results. Efficient data exchange between providers, patients and ancillary services like labs, pharmacies and radiology is a critical component of "meaningful use" compliance. Streamlined access to results can be achieved through an online patient portal that connects directly to the lab.

However, this can be very sensitive patient information – it is imperative that such information only be accessible by the patient or their authorized caregiver.

In order to allow faster patient access to their test results, one organization implemented a system that used both Dynamic KBA and one time passwords, a unique password texted to the patient's phone that expires after a short time. They ultimately found that allowing online access to test results saved them several dollars per transaction in labor, postage and supplies and gave the patients a greater sense of control over their health management.

Telemedicine meets the call for reduced costs. In some cases, patients can be triaged by their primary care team over the phone or through secure messaging via a web portal to determine if the patient needs further evaluation in person. This enables the care team to intervene earlier in a more convenient manner for the patient.

Some progressive providers, particularly those serving niche specialties or rural populations, are using telemedicine to see more patients with reduced staff interaction and cost, while also lessening the burden on the patient. Here, identity management might include a higher level of authentication such as voice biometrics to avoid the possibility that someone could "pose" as a patient.

These combinations can be derived from:

- Something the enrolled user knows (password, pin, challenge question).
- Something the enrolled user has (token, access card, device); or
- Something inherent to the enrolled user (fingerprints, retinal scan, voice print, keystrokes).

In a more robust MFA process, the system might authenticate the user's login by sending a one-time-password (OTP) to the enrolled user's mobile phone that they must then enter into the system to gain access. Or, instead of a OTP, the user might have to use a token or supply a fingerprint.

Making pre-registration worthwhile. Providers benefit by getting patients to complete paperwork ahead of their visit. However, an online pre-registration system that is cumbersome to use may cause users to bail.

Not only that, the needs of the organization may differ according to their level and frequency of patient interaction—the requirements for repeat access at a hospital may be very different than those of a family care physician.

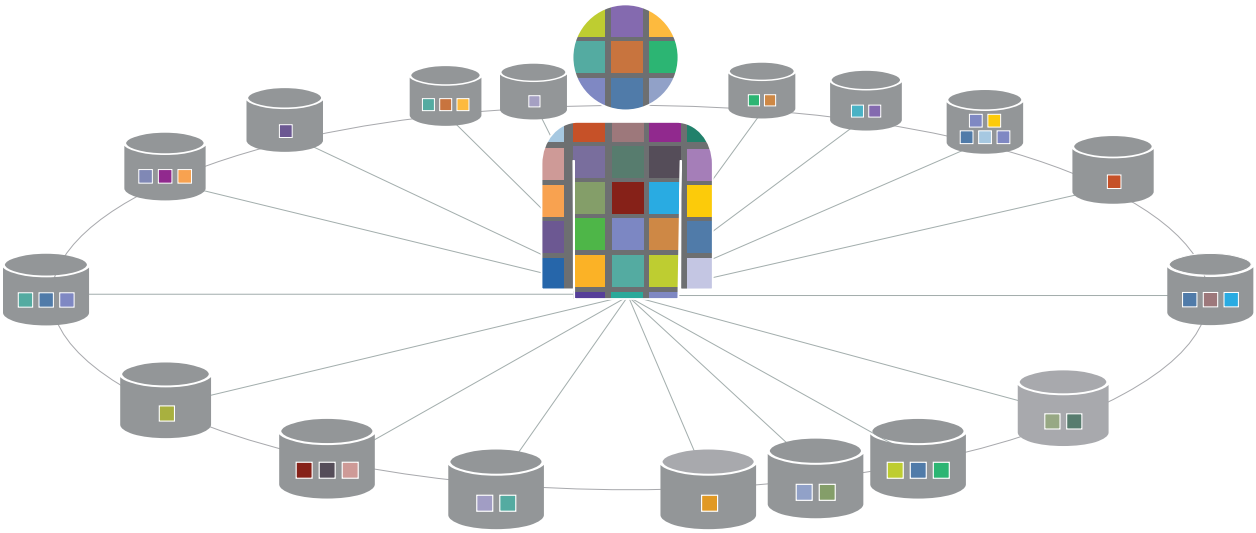
Upon completion of an authenticated enrollment process the patient is issued credentials for future access and can begin the pre-registration process immediately. Because the patient identity has been authenticated upfront, paperwork for subsequent visits can be lessened by the pre-registration system, which automatically pre-fills form information that is not situationally dependent: for instance, demographic information, confirmation of employer and previous health insurance information, and emergency contacts. This provides convenience for the patient through pre-filling forms and saves time for the provider staff by reducing the time on pre-registration calls with patients.

This type of functionality is most practical when a robust authentication program confirms the patient is who they say they are—both upfront, and in each interaction thereafter.

Know your patient, in real time

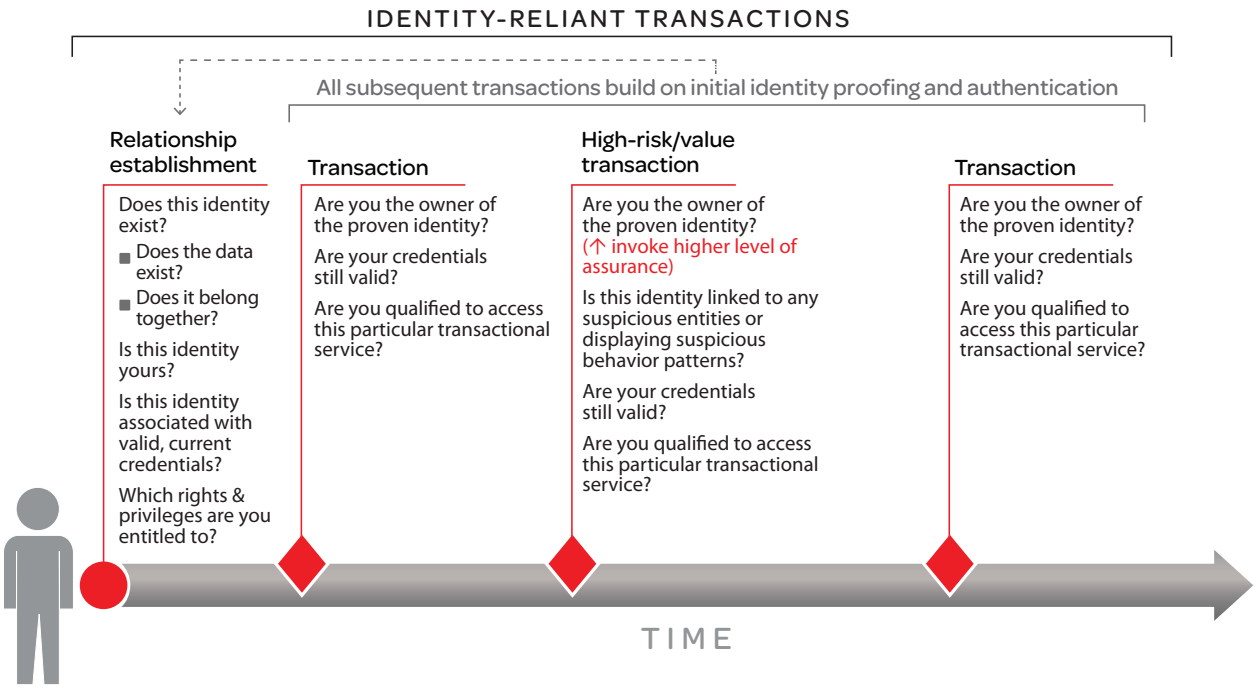
The use cases outlined above all rely on robust identity management systems that bring together, in real-time, data from tens of thousands of disparate sources. The person being ID'd doesn't even have to furnish the information themselves. By having instant access to this multifaceted view of the individual, the organization can verify an identity with 99.9% confidence. What's more, this level of assurance can be achieved for tens of millions of individuals while shielding personally identifiable information from the organization's view – a feature critically important to complying with privacy laws such as HIPAA, HITECH, Fair Information Practice Principles, and other regulations that govern data sharing and retention.

Increasing Volume & Importance of Identity-Reliant Transactions



But simply increasing the pile of "digital DNA" isn't a complete – or effective – strategy. You should carefully consider how the information will be used, and in what circumstances. In other words, ask only what you need to know. For each patient and type of transaction, your ideal identity management solution should determine, in real time, what your organization needs to know to complete the request.

What You Need to Know Changes Throughout Customer Lifecycle



This might cause some heartburn among security personnel who aim to reduce risk by restricting access. But with a flexible, multi-factor authentication program, you can appropriately manage the different types of transactions that occur at various points in patient lifecycles.

Identity Management Fundamentals: An Introduction

The identity management capabilities we've described in this paper can be integrated to existing business applications as callable web services. You can implement them on-site or through a hosted, managed service.

We find that, increasingly, providers are choosing the managed "cloud service" to gain two appealing benefits: 1) It reduces costly data storage and disaster recovery; and 2) it relieves the organization of having to keep up with changing technologies.

Whether installed or hosted, identity management solutions should encompass four technology fundamentals:

At LexisNexis, many of our high transaction volume customers in health care and government do not collect the SSN as an input during their customer enrollment/ onboarding. Even without the SSN, they are able to experience excellent results in uniquely identifying an individual and proceeding to identity verification and/or quiz generation for identity authentication.

1. Real-time access to vast, diverse data sources

The accuracy with which you're able to verify that individuals are who they say they are depends partly on the amount and variety of data your identity management system can access.

Best-in-class solutions offer very wide (diverse) and deep (historical) data. They reach far beyond credit bureau data, standard demographic information and "hot lists" to tap billions of public records from more than 10,000 diverse data sources. They can verify the identities of hundreds of millions of individuals.

In addition, solutions that are connected to such an expanse of data sources can provide more information about each individual. "Out-of-wallet" data points — meaning information not usually carried in an individual's wallet, such as the model of a car the consumer owned during a certain year — can be used to generate a changing set of challenge-response questions for dynamic knowledge-based authentication.

This approach also enables you to achieve the desired level of identity assurance in each instance using the least intrusive form of authentication. In other words, you can avoid asking for sensitive information that seems (from the user's perspective) unnecessary to the process.

2. "Data linking" to connect relevant identity elements into meaningful, purpose-specific views Access to vast quantities of diverse data is only an operational benefit if you can do something useful with it — in the blink of an eye.

A best-in-class solution will not only be able to verify the identity of an individual, but will also have the ability to link familial relationships to the identity of that individual. For example, when requesting a copy of a birth certificate in a "closed record" state, access is restricted to specific familial relationships and/or person(s) acting on behalf of the birth certificate registrant in order to protect the confidentiality rights.

Extended verification of this kind relies on strong data linking capabilities. But data linking is also fundamental to almost all identity management functions. It's the key to turning raw data into information relevant to a particular transaction. And because data linking provides a more complete profile of the individual and a clearer picture of the risk of the transaction, it enables systems to invoke the right measures to achieve the degree of security required in each use case.

In general, your identity management solution should be able to instantly:

- **Locate data relevant to the identity** being presented by the individual.
- **Match data with current consumer inputs.** These might include voluntary inputs like answers to knowledge-based questions, a voice or fingerprint, or a one-time pattern-based PIN, etc. They could also include data about the location and device (IP address, computer settings, etc.) these inputs are coming from. If the location is Los Angeles, for example, is the device actually set to Pacific Time and/or is the browser configured to use English?
- **Normalize and fuse data.** Normalization involves resolving anomalies in data formatting, and eliminating redundancies to improve consistency and cohesion. Data is fused into a compact, highly efficient form for better real-time performance.
- **Filter and organize data into a multifaceted view** that provides what you need to know for this particular transaction with 99.9% confidence.

In some implementations, data linking is all that is required to provide the service requested by an operational system. The identity management solution might return appended data for an online form or a simple binary (e.g., pass/fail or yes/no) authentication result. In other cases, where risk scoring or consumer insights are required, analytics will be applied to the data.

3. Analytics to quantify identity risk and tailor methods to the needed level of assurance

Analytics can detect patterns of behavior, such as suspicious patterns of identity verification failure indicative of fraud or data integrity problems.

In patient identity management, analytics are also used to quantify identity risk by assigning a score representing the level of identity fraud risk associated with a particular transaction. The score is then delivered to the requesting operating system, where your configured rules and thresholds trigger an action, such as accept, refuse review, etc. Scoring of this kind provides an objective, consistent, repeatable way of making high volumes of complex decisions.

Rules that you configure within the identity management solution enable it to make intelligent dynamic decisions about when more information or higher levels of authentication are needed to arrive at your specified level of assurance.

In the case of borderline scores, for example, the system can challenge the person with an additional question, and/or access an additional data source.

4. Multiple authentication factors to meet consumer/constituent needs

In today's dynamic health care environments, organizations that engage in identity-reliant transactions need a high level of security and an equal degree of flexibility to support a wide variety of organizational platforms and end-user devices.

Many applications warrant an identity management solution that enables what we call "variable assertion." This means that the solution supports many different ways for identities to be asserted, verified and authenticated — and that it can apply appropriate degrees of escalated security to different types of transactions. For example, patients in a remote user scenario may present their demographic information, and if the information fails a verification process, the patient may be immediately challenged with a dynamic KBA.

To support different patient needs and preferences requires flexible deployment. Today's best-in-class solutions can provide identity management services simultaneously to operational systems across any number of channels and interact with user devices of all kinds. They can also play within emerging identity management platform architectures, such as OpenID Exchange and Microsoft's Open Identity Trust Framework.

Patient Identity Management: A Prescription for Improving Remote Patient Access

Like a dusty treadmill in a rarely used exercise room, even the most functional EMR won't live up to its promises unless barriers to utilization are lowered and eventually eliminated. Forward-thinking enterprises have realized that thoughtful and proven strategies for identity management are a significant factor in the most effective approaches for achieving widespread meaningful-use, fostering patient satisfaction, enabling secure and convenient patient access, and enabling a more efficient health care delivery system.

For more best practices in identity management contact LexisNexis® Risk Solutions:
Website: http://idmanagement.lexisnexis.com
Email: idmanagement@lexisnexis.com
Phone: 877.221.5292