

White Paper

The Most Important Question in Identity Management for Health Care

Your answer points the way to preventing medical
identity theft and reducing fraud before it happens

June 2012

The most important question in identity management is not: “Who are you?” It’s “What do we need to know about you?”

And nowhere is the answer to that question more critical than in health care, where inadequate systems and processes can not only threaten business integrity and success, but jeopardize lives, as well.

Traditionally papers by identity management providers discuss definitions specific to encryption, issuance of conventional authentication methods, etc. These are important topics, and it is encouraging to see standards emerging that will guide and regulate such practices in a variety of industries.

The purpose of this paper, however, is to shift the focus of the discussion of identity management away from authentication methodology and towards the broader health care context in which identity management is no longer a luxury, but a necessity.

Effective patient/member identity management springs from this fundamental question:

“Given what we are trying to accomplish through this particular transaction, what do we need to know about this individual to insure safety, integrity and trust?”

Or, more elaborately: “What do we need to know to prove this individual is who they say they are and that they are authorized to access the information being requested based on those identity credentials?”

The answer is determined by the intersection of multiple factors: your objectives; product and service characteristics; population demographics and attitudes; the nature, value and riskiness of the transaction being performed; the point in the process and relationship where it takes place; and organizational risk tolerance.

Getting the answer right is critical to the sustainability of health care organizations and, more importantly, the safety of the individuals they serve.

In today’s highly digitized health care information environment, it is incumbent upon stakeholders to look at identity management as both a business problem and a key enabler for core business functions.

“...enables the right individuals to access the right resources at the right times and for the right reasons – a crucial and increasingly business-driven undertaking for any enterprise.”

Gartner, May 2010

Identity fraud is the fastest growing crime in the United States, affecting more than 11 million adults in 2010. Medical identity fraud is the fastest growing type of identity theft. The Ponemon Institute estimates the annual economic impact of medical identity theft to be nearly \$31 billion.

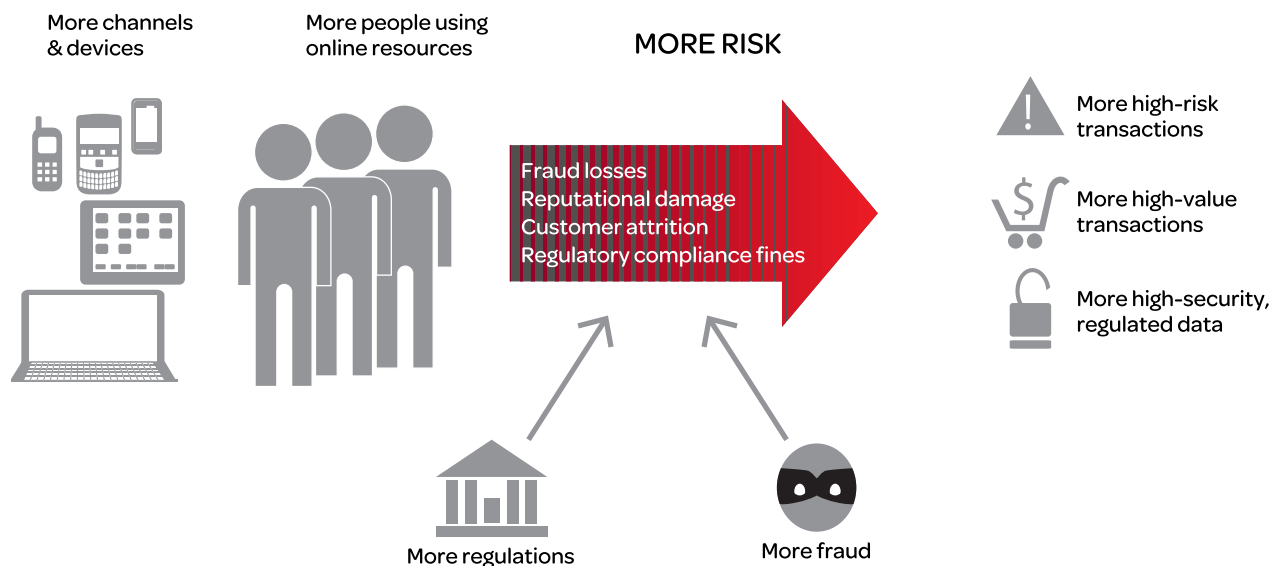
The rapid push toward fully integrated delivery systems, driven by highly mobile and accessible PHI, certainly will be seen by fraudsters as an invitation they can't resist. Moreover, this creates an opportunistic environment for medical identity theft via electronic transactions.

Health care consumers will, and should, expect their data to be secure at all times in order to protect their financial and physical well-being. Health care stakeholders will demand solutions that ensure they are dealing with the right person, at the right time, for the right transaction, thereby minimizing risk and negative impact on their health care delivery decisions, the health of their patients and overall business performance.

For government payers, this means more effective service delivery, the ability to efficiently meet growing demand for services and reduction of unnecessary cost and risk. For private-sector health care stakeholders, it means a potential new source of competitive advantage. As a recent Gartner report states, identity management is "increasingly recognized as delivering real-world business value," and "identity management agility improves support for new business initiatives and contributes significantly to profitability."

Health care reform and heightened regulatory scrutiny have made identity management a top priority within health care organizations and across health information and insurance exchanges. With millions of new consumers entering the health care system and more medical transactions being conducted online, access to a scalable information management infrastructure that can link health information to individuals and identify and authenticate users accessing this protected data is of paramount importance.

Increasing Volume & Importance of Identity-Reliant Transactions



- Prescriptions for controlled substances and the privacy of health care records are examples of internet-available services and information subject to federal and/or state regulation.
- As governments seek to reduce costs, a growing number and range of public services are coming online. Risky transactions include the issuing of credentials such as smart cards for benefits, including Medicaid/Medicare.
- Information that has been readily available in public records, such as Social Security numbers, are a concern given the ease and speed with which they can be harvested via the internet.
- Emerging health care banking boosts the risk even more. By integrating health care payment processes with network access to the banking infrastructure, all the risk factors listed above are combined.

There are tools you can put in place now to meet the increasing demands of identity management.

Enhance existing health care information systems with new identity management capabilities

Identity management is rapidly evolving to encompass these emerging risks and application variability. Outlined below are some of the tools available in the market today.

Point solutions and one-size-fits-all implementations are being supplanted by or absorbed into more comprehensive and flexible approaches. These solutions provide identity management coherency across processes and relationships, as well as identity management consistency across multiple channels and organizations.

At the same time, they enable organizations to efficiently implement a wide range of identity management tools that blend the right identity elements together with the appropriate view and assurance level for each transaction.

Established organizations can layer new identity management capabilities onto existing systems in the form of services. Such services may be added to current operations via an installed or hosted service-oriented architecture.

Merely extending enterprise identity management solutions will not work.

That's because it is difficult to make applications designed for managing only one type of access to internal networks and facilities accommodate the diversity and dynamic nature of payer, provider and health care consumer interactions. These external interactions may occur across the public Internet or the between private networks of individual participants within the health care ecosystem. Such transactions are affected by economic conditions, attitudinal shifts, competitor actions, regulatory initiatives and changing business models.

Moreover, there are some big differences between internal and external identity management:

First, you usually know much less about external users than you do about your own people, who have gone through extensive vetting, often including background screening. That said, more in-depth information on staff is also critical in health care, as medical identity theft often has an “inside” element, such as an employee providing protected information to organized crime rings.

Second, it is nearly impossible to mandate that health care consumers use a specific method, such as smart cards or tokens. If you try to mandate a method that doesn’t feel comfortable or convenient to the end user, they may choose to take their business elsewhere.

These are just some of the challenges of extending enterprise identity management to health care consumer/ constituent transactions. Here are some things that may be more effective:

Three key concepts

These concepts are at the core of the most successful health care consumer identity management solutions. They are general principles shared by diverse business-specific implementations.

1. Identity management is as much about business as about security

Identity validation (or “resolution”), verification and authentication – commonly regarded as security functions – have far-reaching business ramifications. How you perform them can strongly shape your most direct and therefore vital interactions with patients, payers, providers and other health care stakeholders. Thus, while it is important, and sometimes mandatory, to follow industry standards, it is also critical to make sure that the way in which you implement identity management is tailored to your market, business plan and mission to maximize business goals and minimize organizational risk. In other words, there is no “one size fits all” solution to medical identity management.

For example, a major pharmacy that offers an online “prescription center” for refills and transfers, among other services needs to know:

- Is the identity being presented valid? (i.e., it has not been made up or assumed from a deceased individual).
- Can we verify that the applicant owns this identity? (i.e., he or she is not using a stolen or borrowed one).
Does the identity of the individual match the information on file for that prescription?

Compare this with an example of a commonly used health care provider identity verification scenario. When a patient arrives at the health care provider’s building, the registrar or front office staff requests information from the patient, including a medical ID card issued by the health plan, the patient’s driver’s license or other government-issued identification and a description of the chief complaint. The registrar validates the photo on the government-issued identification with the presenting patient, makes a copy of the front and back of the medical ID card and government-issued identification and inserts the copies into the patient record. On subsequent visits, the registrar has an opportunity to compare the presenting patient with the pictures contained in the file to help ensure the patient is who he or she claims to be. While this process is clearly better than a do-nothing approach, it does not offer the most effective or consistent approach to identifying discrepancies or detecting potential fraud.

For example,

- What if a patient doesn't not have his or her medical ID and/or government-issued identification?
- What if the presented information is a made-up or the documentation is forged?
- How does the registrar tie the patient identity to the photo ID if the patient is new and no previous record exists for comparison?
- What if the patient knowingly or unknowingly presents outdated information?
- And what if the patient is attempting to access services or information remotely?

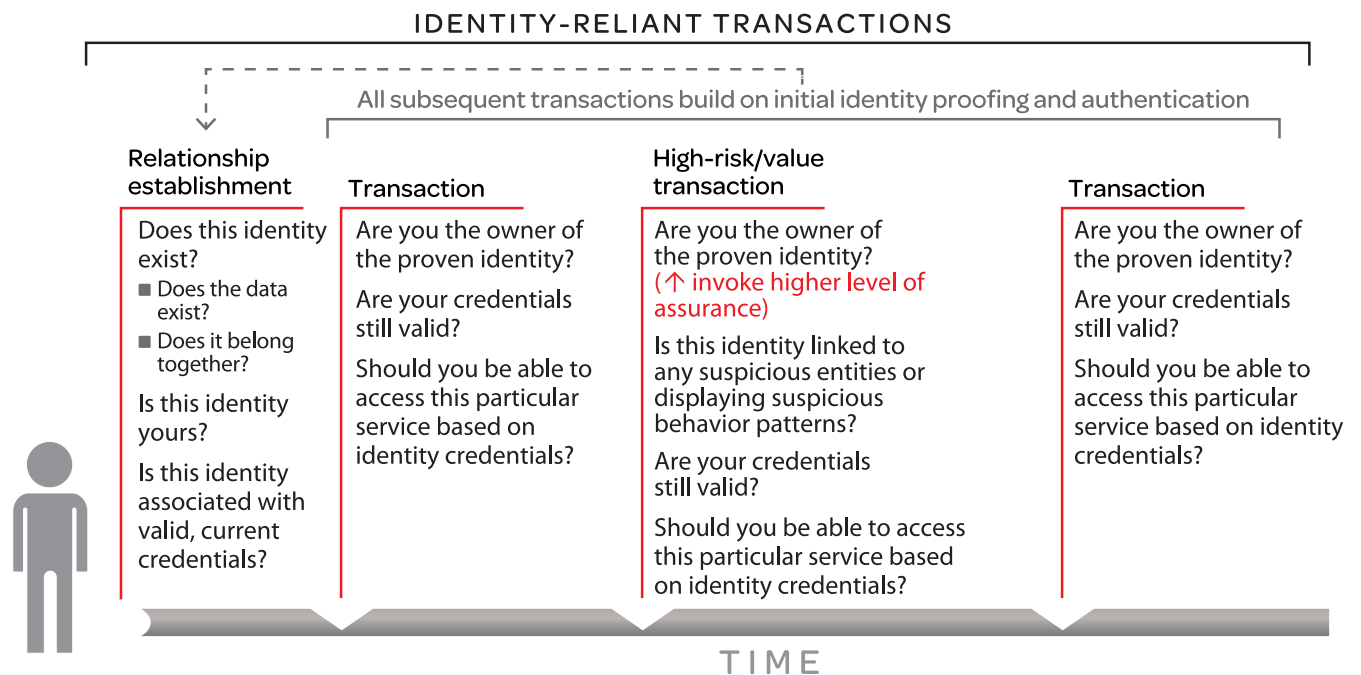
Situations like these compel the health care community to adopt consistent methods and appropriate technologies to mitigate risks involved with identity theft, identity mismatches and poor information collected during the patient access process.

Moreover, what an organization needs to know when it first establishes the relationship can be different from what it needs to know downstream in these relationships.

Parallels and divergences of these examples are obvious as payers, providers, hospitals, health information exchange networks and all other players in the health care strata are charged with managing their specific demographics and populations. In addition, as health care reform drives millions of new health care consumers into the system, accurately linking

Endorsed by the American Hospital Association, LexisNexis Identity management solutions help hospitals and health systems prevent medical identity theft by verifying patient identities in real time during scheduling, pre-registration, or prior to accessing online services. Powerful identity verification and authentication tools deliver instant results to help detect potential fraud and address compliance obligations.

What You Need to Know Changes Throughout Customer Lifecycle



health information to the correct individual will become even more complex, further increasing the risk of fraud and highlighting the need for stringent data security.

For each person being served and each type of transaction being conducted, an organization will need an identity management solution that provides information the organization needs to know in real time. The success of this process depends on the next key concept.

2. “Know your health care consumer” is the point of balance for multiple – and possibly competing - objectives

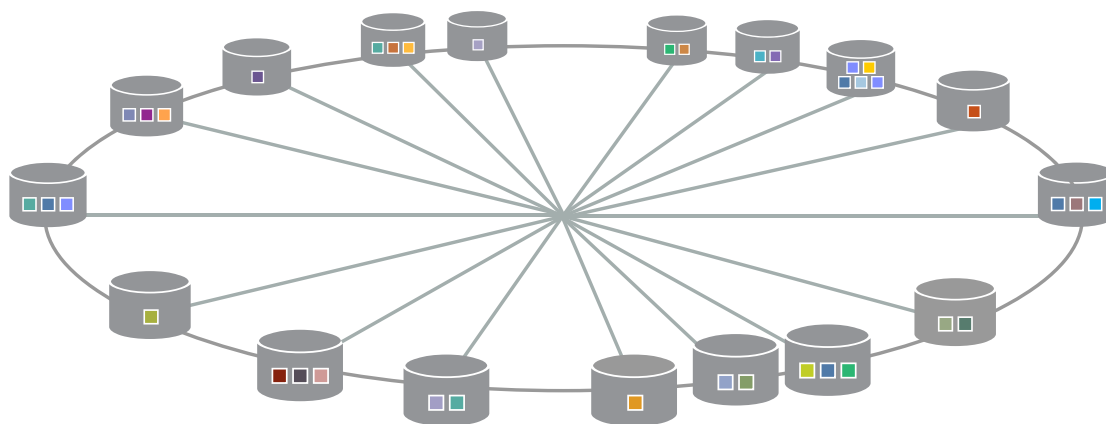
“Know your health care consumer” is a phrase that traditionally has different meanings to health care consumer service than it does for security management. Service people are concerned with raising health care consumer satisfaction by increasing access and ease. Security people are concerned with reducing risk by restricting access.

Effective identity management unifies these objectives. Fusing what you know about your health care consumer from both a service and a security sense enables you to appropriately manage the different types of transactions that occur at various points in health care continuum.

Whether it's a provider retrieving information from a health information exchange, a member using an on-line health benefits enrollment process or an insurer updating a member's file to reflect changes in marital status or the birth of a child, all will need verification for access.

With the number of people in the health care system on the rise, payers need to transform how health information is accessed, exchanged and maintained using robust identity management.

Increasing Volume & Importance of Identity-Reliant Transactions



In real-time, data from tens of thousands of disparate sources can now be brought together to form a multifaceted view that enables businesses and government agencies to resolve an identity with 99.9% confidence. This level of assurance can be achieved for tens of millions of individuals while protecting the privacy of these individuals by shielding personally identifiable information.

The more your identity management service can tell you about your the person whose identity you are verifying, the better you will be able to balance multiple objectives. Knowing more enables you to invoke the right identity management measures necessary to reach your desired level of security for each transaction while at the same time improving your health care consumer’s experience and tailoring service features and offers to fit the consumer’s individual needs.

Knowing more doesn’t mean asking more.

3. Ask for only what you need to know

Knowing more can, in fact, enable you to ask for less information. In identity management industry jargon, the objective is “friction reduction” through “data minimization.” Improve the health care consumer experience by not asking for information you don’t need.

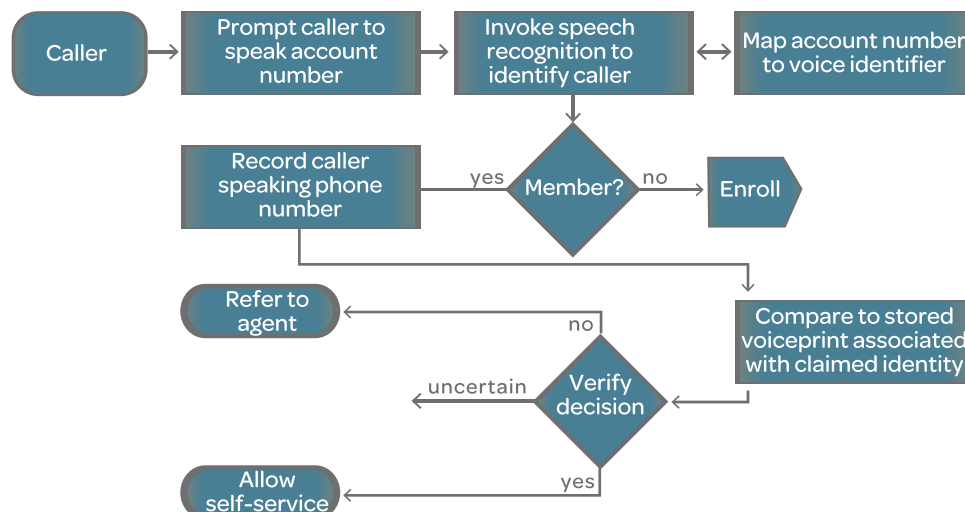
Think about how this principle can streamline online prescription processing.

Low-friction process for physicians. When physicians are enrolled as users of the electronic prescribing network, they are asked to provide their name and state medical license number, as well as providing answers to several knowledge-based questions. An identity management service then verifies the asserted identity and checks to make sure the professional license is current and that the physician is licensed by the US Drug Enforcement Administration (DEA) to prescribe controlled substances.

Because the identity has been proven and linked to authentication factors at enrollment, subsequent transactions are accomplished with ease. When the physician submits a prescription, the system performs an invisible check to confirm that licenses are still valid. This process, which uses DEA-required two-factor authentication, is quick and painless for the physician. For example, in addition to inputting a correct username/password pair, physicians use a hard token as their second authentication factor. Alternatively, the second factor could be a hard-token equivalent (software that generates a one-time password from their smart phone) or a biometric (e.g., a fingerprint or a voiceprint).

Strong security can be, for the most part, invisible to the user. Analytics operating in the background can spot links between health care consumer data and suspicious entities or recognize suspicious patterns of verification failure.

Sample Transaction With Voice Verification



Analytics and be integrated with business rules to adjust the security level and trigger appropriate treatments or approval of treatments. They can also be used to determine if the current transactional pattern of behavior is unusual.

Reacting to health care consumer responses in real time – taking business rules for different product lines, channels and types of transactions, and an entity's tolerance for risk – an identity management service can make dynamic decisions about when to invoke additional and/or stronger measures.

For example:

An online retailer uses identity management to clear more orders and increase customer satisfaction while reducing risk for both fraud and late deliveries. When Jeff purchases a laptop PC at the retailer's site, he pays extra for expedited shipping and enters a delivery address he's never used before, which is different from his billing address. There's no delay in sending out his order, however, because it's not held up for manual review. The identity management service scores the transaction as low for fraud risk because it knows that the device from which he is ordering has been used by Jeff in the past and that the delivery address is a location where he lived until five years ago. (Jeff's mother, intended recipient of the birthday present, still lives there.)

A telecommunications company uses identity management to provide its mobile voice/data customers with superior service. While attending a conference in Mexico City, Rita accesses her mobile phone account management interface to turn on international calling. A single identity-check question pops up on the screen, and, after she answers it, international calling is activated. A few weeks later, she's in Jamaica on vacation and again wants to make international calls. In this case, she receives a one-time password challenge via secure SMS (her preferred form of communication) in order to authenticate her identity before approving her service. The process is conveniently completed and she feels reassured about the security of her account. Rita travels frequently to Mexico City for business, but she's never been to Jamaica – and the identity management service knows it.

As health care moves rapidly toward a retail model and mobile-driven communication, experience from these industries can prove a valuable shortcut to effective business solutions. In the next section, we discuss the technology fundamentals necessary to achieve this kind of powerful, flexible identity management.

Four technology fundamentals

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

An increasing number of organizations are choosing the hosted option. One reason is that businesses are becoming wary of storing personally identifiable health information. They are also aware of the challenges of keeping identity management solutions up to date in markets where attitudes, technology adoption, competitive strategies and business models change frequently.

Whether installed or hosted, health care consumer identity management solutions should encompass the following technologies:

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

The accuracy with which an identity management solution verifies that health care consumers are who they say they are – and the percentage of the population it can accurately verify – depends in large part on the amount and variety of data it can access to provide such verification.

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 thousands of diverse data sources. They can verify the identities of hundreds of millions of individuals.

Solutions with access to such an expansive set of data sources provide more information about each individual. Plentiful “out-of-wallet” data points (information not usually carried in a health care consumer’s wallet), including time-sensitive data (e.g., the model of a car the health care consumer owned between 1995-97), can be used in generating a changing set of challenge-response questions for dynamic knowledge-based authentication.

Fraudsters are increasingly sophisticated in their methods and may try to use information collected from the Internet to answer such challenge questions. Best-in-class identity management services use publicly available data to create a more nuanced picture of the consumer, asking questions such as, “When is the last date you shared an address with this individual?” or “Which of these phone numbers is associated with the address located at 123 ABC Street?” This makes it extremely difficult for fraudsters to use the information they have gathered to pass challenge questions associated with knowledge-based authentication tools. This approach also enables you to use the least intrusive form of authentication required in each instance to achieve your desired level of identity assurance. Because you can achieve a high level of identity assurance by requesting inconsequential information, you can avoid asking for more sensitive information, such as an individual’s.

To further expand your identity solution’s vision, consider participating in a consortium for aggregate-level data sharing with other stakeholders in your health care industry segment or market ecosystem. Advantages include:

- No need to maintain personal health information;
- Ability to enhance your own data with that contributed by other participating organizations; Receive alerts about fraudsters and schemes other entities have experienced that have not yet hit your organization; and
- Improve fraud detection by analyzing additional identity characteristics, such as the velocity with which variations of an identity appear across consortium member data.

If you are interested in this added protection, make sure that you can opt-in as it makes sense for your organization. You may want to participate across the board or just for identity management implementations for certain lines of business or products.

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.

Success Story:

Healthcare remote prescription management

Objective

- Improve accuracy of identity management and ease of use for patients

Solution

- Multifactor authentication
- Something you have: filled prescription RX#
- Something you know: answers to dynamic knowledge-based quiz

Results

- 500,000 patients - identification and generation of knowledge-based questions for 99.5%
- Of patients who were offered the quiz:
 - 90% passed
 - 5% failed
 - 5% opted out

For example, a best-in-class solution cannot only verify the identity of an individual seeking a copy of his or her birth certificate, but the identity of that individual's mother as well. Many state public records agencies are restricted by law to issuing official copies only to those individuals legally authorized to receive them.

Extended verification of this kind depends on strong data-linking capabilities. But data linking is fundamental to all identity management functions. It is 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 instance.

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

- Locate data relevant to the identity being presented by your health care consumer.
- Match it with current health care consumer inputs. These might include voluntary inputs such as answers to knowledge-based questions, a voiceprint or fingerprint, or a one-time pattern-based PIN. They could also include information about the location and device (IP address, computer settings, etc.) from which these inputs are being received. If the individual's normal access 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 it. 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 it 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 health care 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 are mathematical algorithms that examine data and complex data relationships (including the multifaceted views constructed through data linking). Their job often is to detect patterns of behavior, such as suspicious patterns of identity verification failure indicative of fraud or data integrity problems.

In medical identity management, analytics also are 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 you configure within the identity management solution enable it to make intelligent dynamic decisions about when it needs more information or higher levels of authentication to arrive at your specified level of assurance. In the case of borderline scores, for example, the system can challenge the health care consumer with an additional question and/or access an additional data source.

4. Multiple authentication factors to meet health care consumer needs

In today's dynamic environment, health care 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.

Thus, such organizations should choose a solution that enables, in identity management industry terms, “variable assertion.” This means that the solution supports many different ways for identities to be asserted, verified and authenticated, and that it can apply various appropriate degrees of security to different types of transactions. Users, for example, might assert their identities based on something they have (e.g., cell phone), something they know (e.g., password) and/or something they are (e.g., a voice print and a location).

This is the kind of flexibility that is enabling a leading online stock trading and investing company to make a commitment that has become a competitive advantage. This company vows to support any access methods its clients want to use. Period.

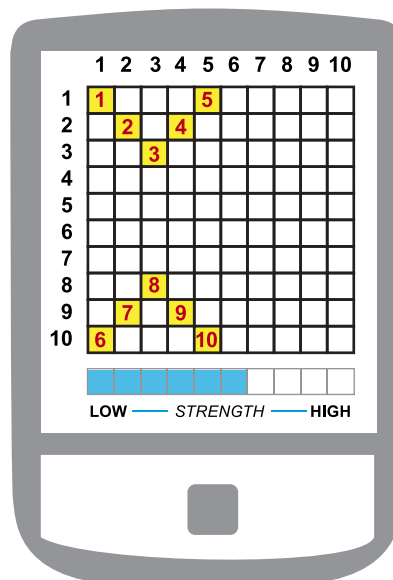
Supporting different health care consumer needs and preferences, you also need flexible deployment. Today’s best-in-class solutions can provide identity management services simultaneously to operational systems across any number of channels and interact with devices of all kinds. They also can play within emerging identity management platform architectures, such as Open ID Exchange and Microsoft’s Open Identity Trust Framework.

Multifactor Authentication With a Mobile Device

This device that users already have on their person can be loaded with software that enables it to perform authentication tasks in a number of flexible ways.

One way is by downloading a PIN-generating mobile client to the registered smart phone. During account set up, users create their own visual passline by clicking squares in the grid.

Later, at transaction time, this passline pattern enables them to respond correctly to a dynamically generated identity verification challenge.



Five Best Practices for Finding Your Answer

Here are some quick takeaways on the steps our consulting teams use to help clients answer the question: “What do we need to know about you?”

- Analyze your objectives and degree of risk tolerance
- Analyze your health care consumers
- Analyze your business processes
- Revisit and reassess your decisions frequently

Conclusion

The number of identity-reliant transactions engaged in across the health care continuum is multiplying rapidly and becoming ever more critical to the success of individual health care organizations. When dealing with any situation involving the sharing of a patient's personal health information it is essential these organizations ask themselves the fundamental question about the individual or entity with whom they will be sharing the information: "What do we need to know about you?"

This question is the starting place for all other questions in identity management. The right answer is the key to making identity management an enabler of great services accessed with ease and delivered at a low cost and minimal risk of fraud.

For More Information

Call 866.396.770, visit lexisnexis.com/risk/HCresources or email us at healthcare@lexisnexis.com

About LexisNexis® Risk Solutions

LexisNexis Risk Solutions (www.lexisnexis.com/risk) is a leader in providing essential information that helps customers across all industries and government predict, assess and manage risk. Combining cutting-edge technology, unique data and advanced scoring analytics, we provide products and services that address evolving client needs in the risk sector while upholding the highest standards of security and privacy. LexisNexis Risk Solutions is part of Reed Elsevier, a leading publisher and information provider that serves customers in more than 100 countries with more than 30,000 employees worldwide.

Our health care solutions assist payers, providers and integrators with ensuring appropriate access to health care data and programs, enhancing disease management contact ratios, improving operational processes, and proactively combating fraud, waste and abuse across the continuum.

We help commercial health insurers, government health care agencies, health information exchanges, as well as hospitals and health systems, maintain trust with members, beneficiaries and practitioners by ensuring only authorized users gain access to personal health information, health insurance programs and provider services. By reducing medical identity theft and protecting access to sensitive information, our Identity management solutions help safeguard reputations and reduce inappropriate utilization of services.

