Health Management Technology
The Source for Information Systems Solutions
January 2006 Issue

Identity and Access Management: the Starting Point for a RHIO

By Jonathan Leviss, M.D.

Regional health information organizations (RHIOs) offer the promise of access to a person's health information whenever and wherever the information is needed. However, public opinion will require that a RHIO maintain a chain of trust with the public, addressing the delicate balance between the availability and security of personal health information.

Jonathan Leviss, M.D., is the medical director at Sentillion Inc., Andover, Mass., and is a practicing physician at the Thundermist Health Center in Rhode Island. Contact him at jonathan.leviss@sentillion.com

People's priorities about the security of health information vary: Some want to keep confidential a medical diagnosis, such as depression, while others do not want to share how much they weigh. Few people want uncontrolled access to all of their health information. How will RHIOs address or prevent the following types of situations and issues:

Example 1: A new physician joins an established group practice. Although admitting privileges at a hospital are granted, he does not yet have access to the community's RHIO. The physician uses a colleague's username and password when rounding on hospitalized patients.

Example 2: Two hospitals that serve the same community have implemented a data interchange capability to share information about patients. At one hospital, caregivers are authenticated using fingerprint biometrics; at the other, caregivers use passwords. A particular patient's data can be accessed by caregivers at both institutions in spite of the different authentication processes. (Scenario described by Dr. David Brailer at the AMIA Spring Congress, 2005.)

Example 3: After reviewing a list of first-grade students requiring a vaccine booster, a school nurse calls a student to her office. She administers a vaccine that was intended for a different student of the same name in another classroom.

Example 4: A state department of health promotes confidential sexually transmitted disease screening for persons 25 and under and funds screening of uninsured persons. After an insured patient is tested, the screening center sends a bill to the carrier. The carrier mails an explanation of benefits to the policyholder, who is the patient's mother.

The Fully Functioning RHIO

To address such challenges, RHIOs must be empowered with basic identity and access management capacities, including the ability to:

- Identify or denote a real-world subject that may be a person, place or thing.
- Verify that when a subject asserts its identity, it is indeed the subject's identity and not that of another subject. For example, the patient truly is Mr. Stevens or the pharmacy to which the prescription was sent is indeed Green's Pharmacy located at 32 Main Street in Providence.

- Create, maintain and remove the identity of subjects. For example, Ms. Gonzalez is admitted to Community Hospital; Dr. Jones marries and changes her last name to Brown.
- Create and maintain relationships between subjects. For example, Ms. Stern is Caroline Stern's mother; Dr. Clark and Dr. Davey are in the same medical practice.
- Allow or restrict what a subject can do. For example, Ms. Stern can review her daughter's health record, or Dr. Tien can no longer access patient records from Community Hospital.
- Track and monitor who uses what information, when and how, including the generation of an audit log to verify that privacy and confidentiality policies are upheld.

In addition to implementing appropriate processes across health systems, a RHIO must apply them differently to various stakeholders with contrasting information needs. Patients need to provide health information to others. Professional caregivers need to review information to treat patients. Family and friends need to provide and review information about a patient's health, often serving as both a patient's medical historian and caregiver. Researchers need to review health information to develop new therapies. Payers need to review information to reimburse for services rendered. Regulators need to review information to ascertain that individuals and organizations are adhering to standards. All of these needs must be served.

Simultaneously, bad people and people behaving badly must be prevented from accessing and using information inappropriately.

Lastly, a RHIO must identify and track complex relationships across the healthcare system. Healthcare relationships include more than people and their care providers. They also include close personal contacts, communities of residence, preferred pharmacies, government agencies that provide research and oversight for healthcare services, and other people and organizations that deliver or support healthcare services. Tracking these relationships will enable a RHIO to support the information services needed by the many members of our healthcare system.

Five Rights for RHIOs

Effective RHIO identity and access management processes involve a five-part life cycle. First, a subject is introduced to a RHIO and is identified, often by an official document such as a driver's license or perhaps the birth of a newborn. Next, the subject is provisioned into the RHIO, assigning a role to the subject such as "hospital patient" or "emergency department physician," and creating relationships to other subjects, such as "mother of Caroline Stern" or "preferred pharmacy for Mr. Stevens."

When the subject interacts with the RHIO, to document new information or to access existing information, the subject is authenticated, asserting that the person is who he or she claims to be. Fingerprint readers, secure passwords and other technologies might support this task. Once authenticated, a subject may view health information, document information or otherwise interact with information services of the RHIO.

Then, technologies control what information the subject may access and what can be done with the information, such as the ability to review a medication list but not the detailed notes of a patient-physician discussion. Ultimately and finally, the RHIO must be able to audit all of the above processes to demonstrate whether or not appropriate information access and use has occurred.

Most hospitals are beginning to recognize that they have not implemented adequate solutions within their institutions to meet these requirements. From the outset, RHIOs must focus on creating effective identity and access management processes across entire communities, often including multiple competing health systems. The first step for a RHIO to successfully execute such a strategy is to hold open discussions with community members. When the public has proof that health information in a RHIO is secure, RHIOs will be effectively positioned to bring unprecedented value to the healthcare delivery system and to communities across the country.