

White Paper



# HIE Provider Verification

The Privacy and Security Elephant in the Room

Michael L. Nelson, DPM

Since patients seek care at a multitude of healthcare settings, their medical information at any one of these locations, by definition, is incomplete. A health information exchange (HIE) is a group of healthcare entities that deploy a combination of policies, governance and technology to facilitate the movement of health data between various stakeholders, including physician offices, clinics, radiology centers, hospitals, labs, pharmacies, etc. These exchanges can be established in and across communities, medical trading areas, states and nationally. The purpose of an HIE is to promote better coordination of care.

ARRA, enacted in February 2009, included significant new investments to encourage the meaningful use of health IT through the HITECH Act. Providers can qualify for federal monies to deploy EHRs only if they can demonstrate meaningful use of the systems. One of the key components of meaningful use is the electronic exchange of health information.

In most cases, HIEs deploy federated models where patient data is fragmented across multiple locations and is maintained under the stewardship of each provider. The compelling value proposition of an HIE is the use of a master patient index (MPI) to aggregate a patient's data from multiple sites in order to view a total consolidated patient record. At first blush, this is a no brainer.

In theory, a patient can visit a provider at any location and his medical record can be quickly and easily accessed. This translates into convenience for patients and the providers; patient safety as a result of a complete patient record, which includes medication history; and cost savings from avoiding repeat lab and radiology results since the initial results can no longer get lost.

However, upon closer examination, patients have deep concerns about

the ramifications of their medical information falling into the wrong hands. Therefore, the federal government, the ACLU and numerous consumer groups have been at the forefront of formulating policy to ensure the privacy and security of PHI and sensitive health information (SHI).

## Privacy and Security

Other than emergency situations where a break-the-glass policy will allow unfettered access to patient information, it is the patient who will ultimately decide who should be granted access to his/her medical information and which information should be shared.

But how will the patient make this determination? The prevailing wisdom is that the patient will seek guidance from his/her primary care physician and trust that advice to grant appropriate permissions to other providers. However, what if the patient does not have a primary care physician, does not have a close relationship with the primary care physician, disagrees with the primary care physician or is being seen by an unfamiliar physician in a hospital, retail clinic or urgent care center? For a patient to make an informed decision about whether or not to share his/her data with a provider, at the very least the patient should know if the provider has an active license to practice and prescribe medication, what his specialty is and whether or not he is sanctioned anywhere in the country.

As the steward of his patient's medical record with full culpability for HIPAA privacy and security breaches, how will the primary care physician determine with whom to share his patient's medical information? The typical criteria will be if he/she knows or knows of the provider seeking access to his patient's information and whether or not the patient's medical condition warrants the sharing of all or part of the patient's medical record. But being familiar with another provider does not equate with knowing his credentials.

Although HIEs are the "middlemen" in transactions between providers, as HIPAA Business Associates they may still be liable for data breaches which compromise PHI and SHI. HIEs have a responsibility to deny exchange authorization and/or data privileges to providers with questionable credentials such as inactive or suspended licenses and sanctions.

The Federal Health Information Technology Strategy for Privacy and Security requires that HIEs: implement security methods to ensure

appropriate authorization and electronic authentication of health information, improve privacy and security protections for health information and prevent unauthorized or inappropriate access.

A number of significant, high-profile data breaches have recently come to light. Under previous HIPAA rule, HHS could not fine healthcare organizations more than \$100 for each violation, and imposed a ceiling of \$25,000 for all similar violations of the same provision. The stimulus made it more expensive for healthcare organizations to breach sensitive health information or put data at risk of unauthorized use. It also sent tiered ranges of escalating minimum penalty amounts, with a maximum penalty of \$1.5 million for all violations of an identical provision.

The most recent privacy and security initiatives focus on access management, which defines and controls role-based access to clinical information, multifactor authentication and digital certificates to confirm a person's identity as part of the identity ecosystem proposed as a national strategy for trusted identities in cyberspace and encryption of clinical data.

However, providers have two identities: a personal identity and a professional identity. Little if any attention has been devoted to real-time provider credentials verification.

## The Trust Fabric

To prevent unauthorized and inappropriate access to PHI and SHI, an HIE must authenticate and verify the credentials of the provider seeking access to that information. Healthcare organizations have greater control over the identity management of their employed providers than of their non-employed providers (i.e., referring providers) and their patients.

This may lead to a false sense of security through a reliance on a trust fabric of provider information across the HIE as recommended by the Privacy and Security Tiger Team of the HIT Policy Committee of the ONC, where each exchange partner is accountable for its exchange transactions and the accuracy of its provider data.

The smaller the geographical area of an HIE, the more reliable the trust fabric. However, as an HIE expands its coverage area, the more "stretched" the trust fabric becomes. And like any fabric, it will eventually tear, increasing the risk of inappropriate access to patient information. As HIEs evolve, they will need some kind of process for a just-in-time enrollment of a provider (i.e., a patient is out of town on business or vacation and visits an unknown provider who is not enrolled in the HIE, but needs to access the patient's information from other providers at that moment in time).

Another potential complication is provider false identity. Anyone with a Social Security number can fraudulently acquire a national provider identifier (NPI) because the National Plan and Provider Enumeration System (NPPES) does not verify that an applicant has a legitimate

medical license. Once a person is assigned an NPI, he/she can fraudulently prescribe medications and bill for medical services. Or, perhaps an unscrupulous person uses the NPI of a recently deceased provider to gain access to HIE transactions.

HIE entities can utilize advanced technologies, such as digital certificates and/or multifactor authentication to authenticate the provider's personal identity. However, this technology, much like the NPPES system, does not verify that the provider's credentials are up to date and credible.

Part of the problem with a trust fabric is that provider data frequently changes, and hospitals typically only re-credential their providers every two years because credentialing is a costly and time-consuming process. Since every hospital has its own time frame for credentialing, Hospital A may credential providers in January and Hospital B may credential its providers in June. A provider may be on staff at multiple hospitals with conflicting profile and credentialing information at each. Which facility has the correct information? In general, providers are very lax about updating their profile information with their multiple trading partners in a timely fashion, because it is time-consuming and labor-intensive.

This holds true even though they are contractually obligated to notify their state license boards, the DEA, CAQH and NPPES, among others, of these changes within 60 to 90 days. As long as the provider's revenue stream and business transaction stream remain uninterrupted, there is no real incentive for the provider to update his records expeditiously.

## HIE Provider Enrollment—Provider Directory vs. MPI

To date, HIEs have resisted the onus of performing provider credential checks, preferring instead to trust their participating provider organizations to take on that responsibility. Rather, HIEs are taking the less complicated path of least resistance by merely creating and maintaining provider directories of participating providers. In light of the fact that HIPAA Business Associates like HIEs are now being held to the same strict standards and culpability of privacy and security as are primary HIPAA entities, such a path is fraught with peril. It is time for the HIEs to rethink their privacy and security strategies.

Provider directories are analogous to local phonebooks. Hospitals, group practices and health plans typically display their directories online and they usually contain address, phone, office hours, education and training. Many of these directories from different hospitals, group practices and health plans in the same locality contain conflicting information about the same provider. The directories do not contain provider credentialing information.

A reliable MPI typically contains primary sourced credentialing information such as state license and DEA status, start date and expiration date; birth date, date of death, education, specialty, board certifications and sanctions in addition to the demographic data found in provider directories.

All of the information is cross-walked with information about the same provider from any of the 50 states. As a result, a single provider golden record will contain state license, DEA

and sanctions information from every state in which the provider has practiced (i.e., therefore, if a provider from Pennsylvania with a clean record logs on to the local HIE for the purpose of conducting clinical data exchange, and a real-time credential check reveals that this same provider lost his license in New Jersey, the HIE may have in place a policy to deny his authorization to utilize the HIE.)

Building and maintaining an MPI is a complex process best left to experienced third parties who could host and maintain it on behalf of the HIE.

Many healthcare organizations misconstrue the CMS NPPES NPI Registry as a reliable source of provider information. However, the only NPI enrollment information that NPPES verifies are the SSN, date of birth and place of birth—none of which do they make available to the public. All of the other information displayed is self-reported and not verified including state license and any other provider identifiers. Furthermore, the registry only lists a primary service address.

A self-contained local HIE such as a hospital integrated delivery network (IDN) which does not consider ongoing provider credential checks to be a necessity, is short sighted. As the National Health Information Network (NHIN) evolves, there will be more and more occasions when information exchange between the local IDN and other providers outside of its medical trading area, perhaps of a national scope, will be commonplace. Preventing inappropriate access to PHI will require access to an MPI.

## The Master Provider Index—Provider Identity Management

Just like patient data, provider data is scattered and stored in multiple, disparate data sources such as medical groups, state license boards, the DEA, NPPES, CMS, Medicaid plans, the Social Security Administration, commercial health plans, PPOs, CAQH, OIG, FDA, etc. In addition, accurate, up-to-date provider data is very difficult to maintain due to license status changes due to moving to another state, retirement, sanctions, death; multiple state licenses; multiple tax ID numbers; new specialties; name changes due to marriage or divorce; multiple addresses in multiple states; address changes; affiliations changes; sanctions assessed. Every month there are data changes for 20 percent of the providers in the United States.

Therefore, each provider record at each data source, by definition, is fragmented and incomplete. Consequently, just as an MPI is included within a health information exchange's architecture, so too should an MPI be a necessary and critical component of an HIE privacy and security infrastructure framework.

The key distinction between a master patient index and a master provider index is that the latter aggregates data from authoritative primary sources—the sources that issue provider identifiers, licenses and sanctions. This authoritative data is the basis for the provider's golden record and enables the master provider index to function as the

provider data source of truth for the health information exchange. Since these primary sources update their files on different time schedules, the master provider index must continuously access data from these sources to maintain the most current provider information. The master provider index is the most effective provider identity management tool available today.

## HIE Provider Verification = Validate Provider Personal Identity + Professional Identity

The HIT Policy Committee unanimously approved the ONC Tiger Team's recommendations that include verifying a provider's identity and allowing providers to delegate the verification process to authorized credentialing service providers.

An HIE should conduct provider verification both at initial enrollment in the HIE and for subsequent transaction requests at a frequency to be determined by the HIE's governing body (i.e., every three months or six months or annually). The ongoing periodic re-verification is important because after enrollment, unpredictably a provider may pass away, retire, move to another state, allow his license to expire and/or get sanctioned.

To prevent inappropriate access to PHI and/or SHI by a provider, an HIE should engage in the following steps:

- 1 Initial Provider Enrollment: Partner with an experienced and reliable third party to store and maintain newly enrolled provider information in a master provider index.
- 2 Verify a provider's personal identity to confirm that he/she is who he/she says he is. This should be done with two factor authentication which requires two of the following: something that the person is (i.e., biometrics), something that the person has (i.e., government-issued ID card) or something that the person knows (i.e., answers to secret questions).

There is available today a Web service which accesses a robust national master provider index and generates provider-specific secret questions. There should be a time limit for answering these questions. The more historical data that is stored in the master provider index, the more granular the questions can be. The question types should be generated in a random fashion so that the same questions are not asked every time. The following are examples of secret questions that can be used: where did you go to medical school, what year did you graduate from medical school, what are the last four digits of your DEA number, etc?

- 3 Verify a provider's professional identity with a real time web-based check of a provider's state license, DEA number, and sanctions status prompted by xml queries to a master provider index that continuously aggregates this information from authoritative primary sources.

## HIE Provider Verification Policies and Rules

Lastly, a health information exchange board must establish policies and rules for provider access restrictions.

For example, how much leeway is acceptable for license and/or DEA

registration expiration? Should you deny access if he is more than a month past the renewal date?

What if the provider answers the secret questions incorrectly? Do you deny access if he missed one out of four questions? Two out of four questions?

What if the provider disagrees with the answers generated from master provider index? How do you resolve the dispute? Will you grant access if the provider is sanctioned in a state other than the one from which he seeks HIE transactions?

Will you grant access if the provider is not licensed in the state from which he seeks HIE transactions but he is licensed in other states? How often should you perform a real-time credentials verification for a given provider? Every transaction? Every month? Every three months?

## Conclusion

As HIPAA business associates, HIEs may be liable for PHI data breaches including inappropriate access to PHI by providers with questionable credentials. Therefore, each HIE should incorporate a master provider index into its service oriented architecture privacy and security framework. The master provider index should be hosted by an experienced, reliable third party which can crosswalk HIE provider enrollment information to the provider golden record. Web service calls to the master provider index should be enabled to generate provider-specific secret questions as part of the two factor authentication of the provider's personal identity and for real time credential checks to verify the provider's professional identity.



**HEALTH MARKET SCIENCE**

2700 Horizon Drive | King of Prussia, PA 19406  
800.593.4467 | email: [info@healthmarketscience.com](mailto:info@healthmarketscience.com)  
[www.healthmarketscience.com](http://www.healthmarketscience.com)

© 2011 Health Market Science. All rights reserved.

HMS Provider MasterFile, HMS Customer Data Integration, CompleteView, CompleteSpend, and Prescriber Eligibility and the Health Market Science logo are trademarks or registered trademarks of Health Market Science in the United States.