FINDING THE RIGHT PARTNER FOR INTEGRATED HEALTH INFORMATION EXCHANGE IN DISCLOSURE MANAGEMENT FIRMS

By Gavin Krumenacker
Vice President of HIE Solutions and Business Development for MRO Corporation
FINDING THE RIGHT PARTNER FOR INTEGRATED HEALTH INFORMATION EXCHANGE IN DISCLOSURE MANAGEMENT FIRMS

Healthcare technology holds the promise of a better tomorrow, and great potential lies in health information exchange (HIE). HIE eliminates boundaries by facilitating the exchange of patient health records between provider organizations, patients and, in some cases, payers to support the Triple Aim of improved population health, improved patient engagement and lower costs.

That’s the vision. In reality, HIE is evolving and many aspects of it remain uncertain. For providers, there will absolutely be a greater ability to share patients’ complete medical histories. Yet, despite the potential benefits, challenges remain—from adopting interoperability standards to safeguarding privacy and security. Many have noted that when it comes to information exchange, healthcare lags far behind other industries such as banking and retail. But, as security expert Gunnar Peterson noted in an interview with CSO Online, the transaction models are entirely different. In finance, he says, there is no gray area about who has the money at any given period of time or where the risk is at any given time. Not so with HIE. When it comes to protected health information (PHI), there is almost no uniformity in how many of these interactions work.

With increased access to PHI comes increased risk. The path forward calls for collaboration between multiple stakeholders in health information management (HIM), risk management, compliance and information technology (IT).

HIE: Not a simple matter of exchange

The idea of HIE has been around for many years and is used as both a noun and a verb, to describe an organization and a process. The United States Department of Health and Human Services (HHS) defines HIE, the noun, as “an organization that provides services to enable the electronic sharing of health-related information.” More commonly, HIE is used as a verb describing the “sharing of health-related information among organizations.”

The process of health information exchange - typically handled by health information management professionals - requires an understanding of complex regulations and operational imperatives, with protection of that information being the most critically important element. The secure exchange of PHI, whether electronic or manual, entails multiple steps of quality assurance to ensure that the right information on the right patient is sent to the right person in just the right format, in order to prevent improper disclosure or even breach.

The impact of improper disclosure and breach

Improper disclosure and breach has significant financial and reputational impacts that may not be obvious but can be very costly. As regulations surrounding the proper disclosure of PHI evolve, the stakes continue to increase for providers and their business associates. The reported incidents of breach escalate as well:

- Since August 2009, more than 500 breaches, involving more than 21 million patient records and at a cost of $4 billion, have been reported to the HHS Office for Civil Rights (OCR), the investigative agency concerned with HIPAA and HITECH Act compliance.
- The number of major breaches of PHI has grown to epic proportions, increasing more than 21 percent in 2012 from the previous year.
- Sixty percent of the incidents were attributed to laptops and other mobile devices, and 20 percent involved business associates.
As exchange through HIEs becomes the standard, it isn’t a question of if a breach will occur but when—and it could be on a much larger scale and with greater frequency.

In addition to increasingly substantial penalties, breaches also impact provider organizations by causing reputational damage, including loss of patients, staff and partners as well as by the related financial and legal impacts from the cost of remediation, potential increases to insurance coverage and costs associated with lawsuits. The American National Standards Institute (ANSI) published a business case for enhanced PHI security in 2012 titled “The Financial Impact of Breached Protected Health Information.” In this study, they identified the following costs when there is a PHI breach:

- Reputational repercussions, including loss of patients, staff and partners;
- Financial repercussions, including costs of remediation, communication, deductible and/or increased insurance coverage, and business distraction;
- Legal/regulatory repercussions, including OCR fines and penalties, state fines and penalties, and costs associated with lawsuits;
- Operational repercussions; and
- Clinical repercussions.

Healthcare organizations that responded to surveys to collect data for the report indicated a wide range of costs associated with each incident of improper disclosure, varying from $8,000 to $300,000. Even at the low end of the spectrum, each time PHI is improperly disclosed there is a financial impact to the organization.

**Evaluating HIE approaches**

To date, HIEs have been developed using a variety of business models, but few have managed to offer both a clear path to financial and operational sustainability.

Many in the healthcare industry have focused primarily on the clinical benefits of HIE for its ability to improve patient care and reduce costs, both of which are critical. Yet given the significant costs of improper disclosure and the number of stakeholders involved in the exchange of health information, hospitals and health systems need to give careful consideration to how they coordinate and govern the availability and required disclosure of PHI. It is in a hospital’s best interest—and clearly should be part of its mission—to protect PHI while optimizing patient care.

Moreover, significant portions of PHI disclosure—typically greater than 50 percent—are to stakeholders outside the scope of most HIE efforts. From an operational perspective, when organizations split responsibility for disclosure across different vendors, they untie traditionally connected processes, which creates risk, confusion and the potential for improper disclosure of health information.

Successful HIE, long term, will depend on the contribution and collaboration of numerous vendors providing different levels of expertise and experience. In short, an “all in” approach will likely not serve the best interests of the entity.

The above factors should be considered while evaluating different approaches for HIE, as well as other pros and cons outlined in Table 1.
# TABLE 1- Approaches for HIE Deployment

## Building a Homegrown HIE
Hospitals can build their own HIE, which is funded and operated by an individual provider organization or group of providers.

**Pros:**
- Organization controls the storage and usage of all data within the network
- Ability to set privacy and security controls

**Cons:**
- Costly
- Entity may not be able to support long term
- Difficult to achieve best-in-class
- Do not provide specific expertise in PHI disclosure

## EMR Vendor Solutions
Hospitals can leverage their EMR’s information exchange modules to share information between providers using the same EMR system.

**Pros:**
- Functionality built directly into the EMR
- Minimal disruption to clinical workflows
- Minimal use of internal technical resources

**Cons:**
- Do not provide specific expertise in PHI disclosure management
- Not an interoperable solution, limited exchange capabilities
- EMRs built to manage clinical documentation, not always comprehensive
- Only supports care-based exchange

## Independent HIE Vendors
Hospitals can contract with independent technology vendors for electronic information exchange.

**Pros:**
- Minimal use of internal technical resources
- Many are startups so the provider has leverage and attention

**Cons:**
- Do not provide specific expertise in PHI disclosure management
- Long-term funding/viability uncertain
- Only support care-based exchange

## Disclosure Management Firms
Hospitals can partner with their PHI disclosure management firms to integrate disclosure systems, processes and governance to achieve compliance with privacy law through HIE while ensuring comprehensive management of disclosure.

**Pros:**
- System agnostic
- Provides expertise in compliance with HIPAA and HITECH Act privacy and security regulations and the hospital’s disclosure policies
- Brings experience in the business of the secure and compliant exchange of health information (manual and electronic)
- Capabilities to implement disclosure and HIE systems across a healthcare enterprise
- Highest degree of governance and risk management
- Supports both care-based and non care-based exchanges

**Cons:**
- Some not established in the HIE space

## Building a Homegrown HIE
Hospitals can build their own HIE, which is funded and operated by an individual provider organization or group of providers.

**Pros:**
- Organization controls the storage and usage of all data within the network
- Ability to set privacy and security controls

**Cons:**
- Costly
- Entity may not be able to support long term
- Difficult to achieve best-in-class
- Do not provide specific expertise in PHI disclosure

## EMR Vendor Solutions
Hospitals can leverage their EMR’s information exchange modules to share information between providers using the same EMR system.

**Pros:**
- Functionality built directly into the EMR
- Minimal disruption to clinical workflows
- Minimal use of internal technical resources

**Cons:**
- Do not provide specific expertise in PHI disclosure management
- Not an interoperable solution, limited exchange capabilities
- EMRs built to manage clinical documentation, not always comprehensive
- Only supports care-based exchange

## Independent HIE Vendors
Hospitals can contract with independent technology vendors for electronic information exchange.

**Pros:**
- Minimal use of internal technical resources
- Many are startups so the provider has leverage and attention

**Cons:**
- Do not provide specific expertise in PHI disclosure management
- Long-term funding/viability uncertain
- Only support care-based exchange

## Disclosure Management Firms
Hospitals can partner with their PHI disclosure management firms to integrate disclosure systems, processes and governance to achieve compliance with privacy law through HIE while ensuring comprehensive management of disclosure.

**Pros:**
- System agnostic
- Provides expertise in compliance with HIPAA and HITECH Act privacy and security regulations and the hospital’s disclosure policies
- Brings experience in the business of the secure and compliant exchange of health information (manual and electronic)
- Capabilities to implement disclosure and HIE systems across a healthcare enterprise
- Highest degree of governance and risk management
- Supports both care-based and non care-based exchanges

**Cons:**
- Some not established in the HIE space
The path forward

Moving forward, the mechanism of health information exchange will be different across recipients, but the governance, operations and tracking of exchange should not be separated.

Regulations governing the disclosure of PHI are continually evolving. Changes in federal law have increased the electronic exchange of PHI while simultaneously tightening controls on how health systems and covered entities conduct that disclosure, and imposing steeper penalties for non-compliance. The risk of breach is further intensifying under the mandates of the government’s meaningful use program that calls for more electronic disclosure and HIE. Most experts agree: improper disclosure or breach is virtually inevitable as we enter the age of HIE.

For these reasons, ensuring the privacy and security of PHI must be top-of-mind when implementing HIE solutions. PHI disclosure management firms have the experience and knowledge of privacy laws and disclosure policies to help hospitals navigate these complex issues. The most technically advanced firms have deep experience in system integrations and electronic delivery, and are building their own HIE solutions that can be easily integrated with EMRs and PHI disclosure platforms. They are a hospital’s best defense against an assault and can minimize damage to an organization and its stakeholders.

Gavin Krumenacker is vice president of HIE solutions and business development for MRO Corporation, based in King of Prussia, Pa.

Footnotes