Understanding the HIE Landscape

Save to myBoK

The health information exchange (HIE) landscape has changed dramatically over the past five years. More HIEs are available to organizations and providers than ever before. Industry initiatives leveraging technological advances and the call for all Americans to have an electronic health record by 2014 will expedite EHR adoption and further efforts in information exchange. A fully longitudinal health record that follows the patient throughout the healthcare continuum will provide clinicians an opportunity to improve patient care.

The speed with which HIEs are developed and implemented across the US will have an impact on the HIM profession. As key stakeholders in efforts such as privacy, security, and confidentiality, HIM professionals will be called on to ensure the appropriate exchange of information. HIM professionals must be prepared to interact and provide guidance to HIEs in order to incorporate foundational information management practices into this emerging arena.

This practice brief describes the current HIE landscape, provides best practices in information management, and identifies how HIM professionals can collaborate with and offer education to HIEs.

RHIO or HIE?

In 2006 the Office of the National Coordinator for Health Information Technology (ONC) began naming, defining, and standardizing information exchange organizations when it contracted with the National Alliance for Health Information Technology to define key health IT terms, including regional health information organization (RHIO).

RHIOs are defined as a group of organizations with a business stake in the improvement of healthcare quality, safety, and efficiency.[1] They continue to serve as building blocks for the Nationwide Health Information Network by sharing information across the Internet.

Other names for information exchange organizations include:

- Health information exchange
- Subnetwork organization
- Health information network

Since ONC released the health IT definitions in 2006, the terms RHIO and HIE often have been used interchangeably. HIE has since been further defined as the electronic mobilization of healthcare information across organizations, communities, or regions.[2] These efforts focus on initiatives such as technology, interoperability, standardization, and harmonization.

HIEs will provide the healthcare industry with the opportunity to electronically exchange clinical information between disparate healthcare information systems, while ensuring the accuracy of the information being exchanged. They provide the infrastructure for secondary use of data for purposes such as public health reporting, clinical quality measurements, biomedical surveillance, and consumer health informatics research.

HIE Governance

The first step in developing an HIE is to establish a governing structure. If the HIE will include facilities competing in the same local or regional market, a structure for building consensus on sharing patient information is imperative.

HIEs may establish a separate organization (profit or nonprofit) with a board of directors. Board membership often includes equal representation from all facilities. However, maintaining the perfect balance of representation may be difficult. A board that is too large to work efficiently and effectively can become paralyzing. In addition, HIE membership may grow with the network's success, so establishing a limit to the size of the board can deter future issues.

The HIE requires a set of bylaws, followed by policies and procedures that are consistent with state and federal law. Formal workgroups that focus on privacy and security, technical, clinical, and financial issues can develop these policies and procedures prior to the HIE's launch.

As no standard governance model exists, healthcare organizations and physicians will require a basic understanding of the HIE governance models specific to them. The "State HIE Toolkit" (http://statehieresources.org) offers a useful resource. Sponsored by ONC, the State HIE Program developed the toolkit to assist in the implementation and development of HIEs. It includes resources such as governance structures, infrastructure requirements, and sample policies and procedures.

Creating a formal leadership structure within the HIE may facilitate further organizational activities such as establishing mission and goals, strategic planning, policies, procedures, and accountability. Important decisions to be made at the initial development of the HIE include opt-in/opt-out models, privacy and security practices, and vendor selection.

Financial sustainability has been difficult to establish for most HIEs, so creating a decision-making process that can be flexible with environmental changes is important. It also encourages ongoing participation.

Opt-in/Opt-out Models

Once governance has been established, one of the first decisions to be made is whether the HIE will have an opt-in or opt-out model.

Within an opt-in model, patients or consumers actively choose to allow their health information to be exchanged with the HIE. The HIE, and therefore the organizations and providers, can presume that every patient made an informed decision to participate. The burden of agreement is placed with the organization or provider, who will ask patients to sign an agreement at the time of treatment.

In this model the HIE assumes that patients will be adequately educated at the organizational level and understand what the exchange of their information means. Organizations must also manage those patients who choose not to share information. Patients who do not want information shared will require organizations and providers to implement policies and procedures that ensure the exchange does not occur.

If relatively few patients choose to participate in the HIE, it is unlikely that its data will become a useful resource. It will not realize the full potential of a longitudinal patient care record designed to improve the quality of healthcare.

In opt-out models, patients must choose to restrict their information if they do not want it shared within the HIE. As a result, the HIE likely offers a greater number of records than it would if it recruited patients individually through an opt-in model.

The HIE still assumes that patients are adequately educated at the point of care and that those who opt out have been adequately educated on the consequences of not sharing information.

A key challenge for both models is communicating the current process for exchanging information. Currently the HIPAA privacy rule allows healthcare facilities to share patient information for treatment purposes with other organizations or providers without a patient's authorization; however, individual state laws may prohibit this exchange.

Consumers may not understand that the HIE provides the same exchange of patient information in a potentially easier format because it combines information from multiple organizations and providers at one time. Thus, patients who elect to exclude their information from the HIE do not prevent their information from being shared; it is just shared in a slower media such as faxes from each individual organization or provider.

Whether the HIE chooses an opt-in or opt-out policy may have an impact on its IT requirements. Thus, establishing the model prior to vendor selection is beneficial.

Vendor Selection

A thorough vendor selection process should include a detailed request for proposal that outlines the HIE's key requirements, such as the opt-in/opt-out model and how the information will be secured. HIM professionals must be involved in order to

clearly define the necessary components. As each HIE is unique, no two HIEs will act or exchange information in the same manner, and each may have different system requirements.

HIM Contributions

HIM professionals can bring a variety of much-needed skills to HIEs. HIE leadership can look to HIM principles to provide support and guidance in the following areas:

- Managing MPI and EMPI data conversions, development, and maintenance
- Developing and implementing HIPAA privacy and security rule requirements
- Developing and implementing HITECH privacy and security rule requirements
- Creating release of information policies, procedures, and practices
- Addressing state and federal requirements for patient confidentiality
- Meeting breach notification requirements
- Integrating data elements from multiple systems, organizations, and providers
- Identifying best practices in information management and records retention

HIM Challenges

In May ONC awarded approximately $550 million in grants to State Health Information Exchange Cooperative Agreement Programs and State Designated Entities as part of the American Recovery and Reinvestment Act (for more on the awards see "ARRA Spurs More HIE Development" below). As a result efforts to establish HIEs are accelerating.

Several information management challenges within the HIE environment will remain constant, regardless of the governance structure. To that end, each HIE should have an established HIM department designed to implement, maintain, and manage all protected health information exchanged.

HIM challenges occur as the need to coordinate and convene the HIE is balanced with the need to fully define and execute information management policies and procedures. Current HIE state-level priorities should include the development of consistent policies, application of standard practices, and implementation of interoperability standards.

In addition, many of the challenges that HIEs will encounter are the same challenges that HIM professionals currently encounter on a daily basis. Challenges such as patient identification management, privacy and security, and release of information (ROI) will need to be addressed.

HIEs have the added responsibility of business associate requirements under HIPAA and specific priorities to develop appropriate safeguards for access, use, and control of patient data. HIEs should rely on the expertise of HIM professionals to help formulate these policies and procedures.

AHIMA component state association leadership should seek out opportunities to collaborate with HIEs and discuss how HIM professionals can assist with many of the challenges the HIE will encounter. Appendix B outlines a sample CSA HIE position description. Appendix C offers a list of HIM talking points for HIEs.

Patient Identification Management Challenges

Patient identification management is a critical process for HIEs. If a patient is not identified the same way in all the systems integrated within the HIE, there is a high risk that duplicate record numbers for that patient will be created. If each organization contributing data to the HIE has a 10 percent error rate in MPI data elements and 50 organizations and physicians contribute to the HIE, the corrupt data could be staggering.

Patient identification management efforts should include ensuring the right patient is identified when two patients with the same name are included in the database. The HIE must ensure that MPI software algorithms implemented to identify potential duplicates are sophisticated enough to identify and resolve duplicates, overlays, and overlaps.

Similar to good MPI management procedures within an organization, HIEs should use front-end software applications with rules-based logic that provide an alert or stop mechanism before integrating data if an entity submits data to the network that are incomplete, in an incorrect format, or have the potential to create a duplicate record.

HIEs must consider other patient identity issues such as lack of standardized naming conventions among hospitals, communication of organizational patient merges, and individual system limitations at both the HIE and organizational level. HIM professionals are an excellent candidate and resource to map out how patient identification management and maintenance is carried out at the organizational and HIE level as well as defining common processes, data elements, and information management best practices necessary to support the integrity of patient information.

It is a given that duplicates and variations in naming conventions will occur. The challenge for HIEs will be managing these issues effectively.

The State of HIE: 2010

A 2010 report from eHealth Initiative found that the number of HIEs is increasing, as is their impact on providers and organizations. It found:

- The number of HIE initiatives continues to grow, with 73 initiatives operational in 2010 (up from 57 in 2009).
- There is a small but critical mass of sustainable organizations.
- Health information exchange initiatives do not have to have a financial relationship with or partially own the organizations involved in order to become sustainable.
- More organizations are reporting a reduction in staff time and redundant testing through the use of HIE.
- New challenges are rapidly emerging related to federal policy and governance of health information exchanges.
- Patient engagement has increased dramatically. More organizations are providing services to patients and providing access to patient data through health information exchange.
- Initiatives are creating methods to address the complexities of security and privacy. More organizations are creating systems that allow patients to control the level of access to their information.

Source: eHealth Initiative. "The State of Health Information Exchange in 2010: Connecting the Nation to Achieve Meaningful Use." 2010. Available online at www.ehealthinitiative.org/uploads/file/Final%20Report.pdf.

Privacy and Security Challenges

According to research from RTI International, the biggest challenges to establishing an HIE are varying interpretations and applications of HIPAA privacy and security rules, inconsistencies between state and federal privacy laws, and lack of trust.[3]

The lack of a clear and consistent HIE approach to privacy and security may hinder the US's ability to realize the benefits of electronic health information exchange.

In an effort to bridge the gap on privacy and security within HIEs, ONC published "The Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information" in 2008. The framework was based on a review of numerous domestic and international privacy and security documents and practices.

The report outlines eight principles that public and private-sector entities should use when engaging in electronic HIE. The framework also includes compliance and enforcement approaches.

The principles are designed to complement current state, federal, and local laws and regulations. They provide detail on such issues as individual access, correction, openness and transparency, individual choice, collection, use and disclosure limitation, data quality and integrity, safeguards, and accountability.

HIM professionals have a responsibility to develop and implement system-wide policies and procedures that address the privacy and security of all individually identifiable health information, regardless of the medium used to capture, store, and transmit information.

Release of Information Challenges

Release of information that promotes HIE is an essential function to the delivery of healthcare. Information must be provided completely and timely to care providers for its intended purpose. However, today's complex medical and legal environment does not always provide clear and concise guidelines for release of information.

Currently, many laws and regulations govern how, when, what, and to whom protected health information is released. The HIPAA privacy rule and HITECH Act contain specific requirements for the management of personally identifiable health information to balance the confidentiality of the individual with the need for complete and timely exchange of health information.

Confusion occurs when state laws are added to the process. States have their own varying privacy regulations, and HIEs have the burden of understanding and navigating many different and potentially conflicting requirements-especially if the HIE provides services to multiple states. State laws can also vary in focus and strictness of patient privacy.

HIEs must manage the overall ROI process in order to ensure confidentiality, security, and compliance in releasing protected health information. It will be crucial for HIE policies and procedures to include the practices that support the ROI process of disclosure and its oversight.

HIM professionals should be aware that not all HIEs will provide traditional ROI services (e.g., releasing complete health records to the Social Security Administration for disability determinations). Some may choose to allow the source system at the organization or provider level to be responsible for meeting this type of request. The HIE may limit ROI functions to patient care requests (e.g., one organization to another or organization to provider).

Regardless of the ROI model adopted, each HIE should have a clear understanding of the consent requirements for the appropriate release of information.

Current industry activities such as tracking disclosures will also have an impact on organizations and HIEs alike. HIM professionals should be prepared to assist HIEs in developing and maintaining sound ROI processes to ensure appropriate disclosures.

Breach Challenges

Breaches are defined under the HIPAA privacy rule as an impermissible use or disclosure that compromises the security or privacy of protected health information such that the use or disclosure poses a significant risk of financial, reputational, or other harm to the affected individual. The HITECH Act revised the HIPAA provisions (effective September 2009) and required business associates to comply with breach notification requirements.

As such, organizations or providers (covered entities) participating in an HIE (business associate) should have an appropriate business associate agreement in place that clearly outlines breach notification requirements.

The HITECH breach notification regulations require covered entities and business associates to promptly notify affected individuals of a breach. They must also report breaches to the Department of Health and Human Services and notify the media of breaches involving more than 500 individuals. Business associates must notify covered entities of any breach involving the business associate.

The new regulations place an additional compliance burden on HIEs, in that these organizations are now subject to the civil and criminal penalties associated with breaches. The HHS secretary is authorized to conduct compliance audits and use civil enforcement provisions, provided no criminal conviction is associated with the breach. However, if willful neglect is proven the secretary is required to impose civil penalties.

Consumer fear of potential data breaches could provide another hurdle in information exchange. A data breach could be financially devastating as HIEs begin working with organizational business associates and providers.

HIEs must include appropriate safeguards against potential breaches, including:

- Releasing PHI in accordance with privacy rule requirements
- Protecting electronic information per the security rule requirements
- Ensuring staff are properly trained on privacy and security rules
- Abiding by minimum necessary requirements
- Securing computers through appropriate access policies and procedures.

They also must be prepared to investigate and report if a breach does occur.

Correction Challenges

Correcting electronic health information can be a struggle for any organization. System limitations and functionality often dictate who, when, and how corrections can be made. However, HIPAA states that individuals should be provided with a timely means to dispute the accuracy or integrity of their individually identifiable health information and have erroneous information corrected or have a dispute documented if their request is denied. Covered entities have 60 days to correct the record or notify the individual the request was denied.

Covered entities must ensure that corrected information is provided to anyone who may have received the erroneous information, including HIEs. Challenges occur when corrected information is not sent to others, source systems are not identified at an organizational level, or the HIE agrees to a correction that an organization may have previously denied.

Clear and concise policies and procedures are required at both the organizational and HIE levels to ensure that corrections are handled in an appropriate manner. Corrections will depend on HIEs and their agreement with the hospital or provider. At a minimum the policy should clearly state who can initiate a correction and who is required to notify whom and within what time frame.

For example, hospital A requires that all requests for amendments/corrections to health information be submitted to the ospital within five business days. The HIE is not allowed to independently and arbitrarily make patient amendments to health information.

As the HIE will most likely not be the source system for the health information, corrections in this environment can be risky. Organizations should understand how corrections will be made by the HIE when the healthcare organization has agreed to make corrections in the patient's health record. The change has to be made to all copies of the health record across the continuum of care. HIM professionals can provide leadership and guidance regarding HIPAA privacy rule amendment requirements for the organization and HIE.

Audit Challenges

Auditing record access within the HIE requires HIM expertise during vendor selection, implementation, and ongoing practice. HIM professionals are responsible for ensuring a safe and secure environment for patient information, and confirming this environment exists requires that systems offer detailed audit monitoring capabilities.

HIM professionals can help outline the desired audit functions during vendor selection. Once these audit functions are understood, the work begins. Policies and procedures addressing appropriate role-based access levels must be established to serve as a baseline for an auditing policy and procedure. A system then needs to be established to perform the auditing. This can be a time-consuming, complicated task with multiple users and facilities.

Although a challenge, excellent auditing capabilities in an EHR can provide a sense of security for patients, which will assist with their adoption and acceptance of an HIE.

ARRA Spurs HIE Development

On May 13, 2010, ONC awarded approximately $550 million in grants to State Health Information Exchange Cooperative Agreement Programs and State Designated Entities as part of the American Recovery and Reinvestment Act of 2009. (A full list of programs is available in appendix A in this online version of the practice brief.)

These programs will promote HIE based on the collection of standards, requirements, and protocols of the Nationwide Health Information Network. The NHIN will provide a nationwide secure infrastructure to connect organizations, providers, and consumers to interoperable health information across cities and states.

This critical initiative of the national health IT agenda is expected to provide patient information to the right provider on the right patient at the right time and support ongoing efforts to improve the healthcare delivery system in the US. Speaking at an IT conference in April 2010, David Blumenthal, national coordinator for health information technology, stated, "What we want is a robust exchange [of health information], not a single solution," referring to a system that would be tailored to regional capabilities for information exchange around the country.[1]

Current industry initiatives such as those defined within ARRA will certainly positively affect information exchange in the US. Meaningful use criteria under ARRA include requirements that organizations and providers use certified EHR technology that can accommodate the electronic exchange of information. Meeting this requirement will assist providers and organizations in qualifying for Medicare and Medicaid incentives by demonstrating meaningful use.

References to information exchange can also be found within HITECH regarding revisions to agreements between covered entities and their business associates. HITECH requirements necessitate a business associate agreement between organizations and HIEs and breach notification safeguards in these relationships.

On April 8, 2010, AHIMA responded to the Health Information Technology Certification Programs Proposed Rule. AHIMA recommended that ONC continue efforts to certify health IT beyond EHR systems to include HIE. These current industry efforts will no doubt place a spotlight on HIE activities and the organizations seeking meaningful use incentives and EHR adoption.

Note

1. Mearian, Lucas. "Health IT Funding to Create 50,000 Jobs." Computerworld, April 30, 2010. Available online at www.computerworld.com/s/article/9176157/Health_IT_funding_to_create_50_000_jobs.

HIM Responsibilities

The HIM profession is changing. HIM roles and responsibilities are moving forward as advancements are made in healthcare delivery systems. Solid information management practices at the HIE level are vital to an HIE's success. HIM professionals can facilitate the design and maintenance of privacy and security practices, record retention activities, release of information activities, and other fundamental core competencies of the profession in both new and established HIEs.

HIM professionals should be involved at the workgroup and board level within an HIE. HIM professionals, healthcare organizations, and physicians must work with component state associations to support the establishment of the HIE, develop HIE policies and procedures, and incorporate fundamental information management principles into HIE functions.

Notes

1. Healthcare Information and Management Systems Society. "Healthcare Information Exchange." Available online at www.himss.org/asp/topics_hie.asp.

2. Ibid.
3. RTI International. "States and Territories Begin to Reduce Challenges to Electronic Health Information Exchange." August 1, 2007. Available online at www.rti.org/news.cfmnav-7&objectid=D7331450-F4ID-435A-84CA2FAA80518822.

Resources

AHIMA. "AHIMA Comments, Testimony, Analysis, Correspondence & Resources."

AHIMA. "Health Care Reform and Health IT Stimulus: ARRA and HITECH."

AHIMA. "Managing the Integrity of Patient Identity in Health Information Exchange." *Journal of AHIMA* 80, no. 7 (July 2009): 62–69.

AHIMA. "Reconciling and Managing EMPIs." *Journal of AHIMA* 81, no. 4 (Apr. 2010): 52–57.

Cassidy, Bonnie S, Elaine King, and Vicki Wheatley. "ARRA's Impact on HIM." *Journal of AHIMA* 81, no. 2 (Feb. 2010): 48–49, 56.

Department of Health and Human Services (HHS). "Health IT Policy Committee (A Federal Advisory Committee)." Available online at http://healthit.hhs.gov/policycommittee.

HHS. "Nationwide Health Information Network (NHIN): Overview." Available online at http://healthit.hhs.gov.

HHS Office of the National Coordinator for Health Information Technology. Available online at http://healthit.hhs.gov.

HHS Office of the National Coordinator for Health Information Technology. "The Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information." Available online at http://healthit.hhs.gov.

Appendixes

Three appendixes are included in this online version of this brief, available in the AHIMA Body of Knowledge at www.ahima.org:

- Appendix A: State Health Information Exchange Cooperative Agreement Program
- Appendix B: Volunteer Position Description for CSA Health Information Exchange Representatives
- Appendix C: Talking Points for HIM Professionals

Prepared By

Susan Carey, RHIT, PMP
Michelle O'Connor, MPH, RHIA, FAHIMA
Traci Waugh, RHIA
Lou Ann Wiedemann, MS, RHIA, FAHIMA, CPEHR

Acknowledgments

Lorraine Fernandes, RHIA
Teresa Hall, RHIT
Aviva Halpert, RHIA, CHPS
Susan Torzewski, RHIA
Allison Viola, MBA, RHIA
Diana Warner, MS, RHIA, CHPS

The information contained in this practice brief reflects the consensus opinion of the professionals who developed it. It has not been validated through scientific research.

Article citation:
AHIMA. "Understanding the HIE Landscape." *Journal of AHIMA* 81, no.9 (September 2010): 60-65.