Understanding the HIE Landscape

The health information exchange (HIE) landscape has changed dramatically since HIE and the Nationwide Health Information Network (NwHIN) was first conceptualized in 2001. The National Committee on Vital and Health Statistics (NCVHS) published recommendations in 2001 on nationwide electronic health information exchange in the report titled "Information for Health, A Strategy for Building the National Health Information Infrastructure." Formally codified by the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, the Office of the National Coordinator for Health IT (ONC) has supported the development of standards, services, and policies for HIEs. The number of HIEs and HIE stakeholders exchanging information has grown exponentially as a result of ONC's efforts.

But both emerging and established HIEs continue to face challenges and barriers, such as:

- Financial sustainability
- HIE governance
- Winning stakeholder support
- Establishment of consistent privacy and security safeguards

In spite of the numerous challenges, the promise of improved patient care resulting from the availability of a longitudinal health record across the healthcare continuum provides the necessary incentive to continue working toward accurate, secure, and interoperable health information exchange.

The speed with which HIEs are developed and implemented across the US has impacted the health information management (HIM) profession. As key stakeholders in efforts such as privacy, security, and confidentiality, HIM professionals will be called upon to ensure the appropriate and accurate exchange of information. HIM professionals must be prepared to interact and provide guidance to HIEs in order to incorporate foundational information management and governance 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.

HIE Growing in Demand

The introduction of payment and delivery reforms, which range from the establishment of accountable care organizations (ACOs) to bundled payments and patient-centered medical homes, is creating a compelling business case for electronic exchange. In response to HIE-infused initiatives like the federal government's "meaningful use" EHR Incentive Program, healthcare systems and small providers now desire to link to an HIE. Innovative approaches to electronic information exchange are emerging as a result, including private HIE networks advanced by hospital systems pursuing ACO status, exchange services offered by electronic health record (EHR) vendors, and regional- and state-level information exchange initiatives. According to a recent KLAS survey, the number of active private HIEs tripled from 52 in 2009 to 161 in 2010.[1]

Instead of waiting for state HIEs to mature, some larger health networks have begun contracting with IT vendors to develop their own proprietary health information exchanges focused on exchanging information between its own facilities and select outside partners. Concerns have been raised that, because of their narrow focus on providing services based on margin and competitive advantage, such private HIEs will drain customers and resources away from state and community HIEs.

State and community HIEs have seen a steady-although less dramatic-rate of growth. The eHealth Initiative (eHI) identified 255 HIE initiatives in 2011, up from 234 in 2010. Many HIE proponents are concerned that the rapid growth of private HIE activities will ultimately undercut the state and community HIE business model, decreasing the likelihood of their success and making the NwHIN dependent on nascent technologies for community-level functions, such as record locator services.

For the time being, ONC has adopted a wait-and-see attitude, contending that different models work best for different states. ONC has urged its grantees to try to leverage the private HIE development in their states, looking for ways to provide services not being offered by the private HIEs, such as linking private HIEs together, providing access to rural providers, or offering

unique services as a platform through which innovative software developers could offer valuable new services to healthcare providers and other HIE participants. Other possible services include patient locator services, immunization registries, birth registries, and cancer registries. Proponents of state and community HIEs believe they are uniquely positioned to bring competitors together to achieve unmet service needs.

NwHIN Activities and Differences

The NwHIN, the former NwHIN Exchange (now called eHealth Exchange and operated by a public-private partnership), and The Direct Project are three initiatives launched to help expand secure HIE efforts using NwHIN standards.[2] If NwHIN is considered as the "Internet"-an electronic environment in which the use of a common set of standards, services, and policies will allow a group of entities to exchange information, then eHealth Exchange could be compared to a consortium using a secure "intranet" in which only approved members can gain access after receiving the appropriate security credentials and agreeing to the terms of use.

The Direct Project is similar to secure e-mail or secure instant messaging. The NwHIN comprises multiple approaches one could use to electronically exchange health information among a variety of stakeholders. The variety of approaches to exchanging information may lower the cost of connections between providers. For example, Direct allows information to be pushed between providers and eliminates the cost of interfaces. The Direct Project specifies a simple, secure, scalable, standards-based way for participants to send authenticated and encrypted health information directly to known, trusted recipients over the Internet.

Direct Project and CONNECT Differences

What is the difference between the Direct Project and CONNECT?

The Direct Project specifies a simple, secure, scalable, standards-based way for participants to send authenticated, encrypted health information directly to known, trusted recipients over the Internet.

CONNECT is open source software that can be used for local or nationwide health information exchange. CONNECT uses Nationwide Health Information Network standards and governance to make sure that health information exchanges are compatible with other exchanges being set up throughout the country.

If NwHIN is considered to function like the Internet, then Direct is the secure e-mail and CONNECT is the open source software used for the exchange of health information.

Consent and Directed Exchange

An ONC Privacy and Security Workgroup, known as the Tiger Team, recommended that fair information practices (FIPs) be followed.[3,4] Because information sent from provider to provider is encrypted, directed exchange for treatment does not require patient consent beyond that which is already required in current law or has been customary practice. The Direct Project does not include complex patient scenarios, such as an unconscious patient brought to the emergency department. Rather, it is meant to be applied to the transport of health information from one provider to another, such as to facilitate the exchange of information for a patient seeking an opinion from a specialist.

For some providers, these communications are part of satisfying stage 1 meaningful use objectives. The Direct standards and services can be implemented by any two participants, organizations, or a community without a central governance structure. Each Direct user is provided with an e-mail address to push the relevant medical information to another user, using Internet standards.

CONNECT is open source software that can be used for local or nationwide health information exchange. CONNECT uses NwHIN standards and governance to make sure that health information exchanges are compatible with other exchanges being set up throughout the country.[5]

- The software provides the ability to locate patients, request and receive documents, and record the transaction for subsequent auditing by patients and others. Other features include mechanisms for authenticating network participants,

formulating and evaluating authorizations for the release of information, and managing patient preferences for sharing information.

- More than 20 federal agencies collaborated to build CONNECT to tie their health IT systems into the NwHIN.
- Any organization can download and use the CONNECT solution without a fee.
- Seven federal agencies have demonstrated the feasibility of sharing data with each other and with private sector organizations using CONNECT; in addition, multiple states, private sector organizations, and health IT vendors have begun piloting the software.
- Security or the "trust fabric" is provided by the combination of the NwHIN operating procedures, and the data use and reciprocal sharing agreement.[5,6]

CONNECT solution is moving to a public/private governance model. Healtheway will operationally support the eHealth Exchange by onboarding new participants, conformance and interoperability testing, and operating policies and procedures. By transitioning to Healtheway, a public-private partnership, the goal is to create a sustainable business model. Initially, CONNECT was built as a single solution to allow federal agencies to tie their health IT systems into the Nationwide Health Information Network.

A collaborative approach was adopted to drive down development costs for each agency and ensure a solution was available that met federal regulations and requirements for health IT interoperability. Because CONNECT is built as an open source software, it has been made available for use throughout the healthcare industry. This helps to fulfill an added objective for CONNECT, which is to serve as a platform for innovation. The solution can be downloaded for free, and the industry is encouraged to download it, improve upon it, build additional solutions with it, and resell the product into the public and private sectors.

Nine Principles for NwHIN Governance

1. Transparency and openness
2. Inclusive participation and adequate representation
3. Effectiveness and efficiency
4. Accountability
5. Federated governance and devolution
6. Clarity of mission and consistency of actions
7. Fairness and due process
8. Promotion and support of innovation
9. Evaluation, learning, and continuous improvement

HIE Governance Assures Continuity

Governance is the mechanism that assures necessary policies, standards, and services are in place so organizations can manage business operations, services, and relationships with its stakeholders. This ensures the organization is appropriately established, coordinated, and overseen, and that its policies are enforced.

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 (either 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.

Enacted in February 2009, HITECH requires the ONC to establish a governance mechanism for the Nationwide Health Information Network.[7] It also authorizes the Federal Health IT Policy Committee to recommend the areas in which standards, implementation specifications, and certification criteria are needed for the electronic exchange and use of health information.

The NwHIN should be:

- An environment of trust and interoperability for exchange based on NwHIN Conditions of Trust and Interoperability (CTEs)
- The preferred approach for exchange of health information nationwide
- Supported by the federal government with strong incentives to vigorously promote adoption

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.

In May 2012 the ONC issued a request for information (RFI) public comment period seeking input on a broad range of governance mechanisms. In response to the public comments received, ONC decided against issuing a formal regulatory governance structure and instead proposed the following four-step non-regulatory approach.

- **Lead Through Action:** Use available levers to directly accomplish specific goals
- **Lead Through Guidance:** Disseminate a framework of principles and-where available-good practices, models, and tools for specific exchange challenges
- **Engage, Listen, and Learn:** Proactively encourage and engage with communities and stakeholders offering solutions for exchange
- **Monitor:** Monitor marketplace for abuses, exchange successes, gaps, and failures as well as consumer and provider attitudes

Opt-in and Opt-out Models

The healthcare industry has long debated what consent is required, or best, to transmit health information through an HIE. Consent models for health information exchange are often referred to as either opt-in or opt-out. Patients given the opportunity to **opt-in** to HIE may sign a state-defined consent form or give consent via an online patient portal. In the opt-in model, the patient must proactively agree to participate in the health information exchange before information is shared.

Patients given the opportunity to **opt-out** of a health information exchange must actively choose not to participate in the health information exchange by signing an opt-out form or through patient mailings/brochures, posted notices, or an online patient portal. The patient's health information is exchanged through a network unless the patient formally elects to opt-out. Opt-out models typically exclude specially protected health information such as psychiatric records or drug and alcohol treatment covered in 42 CFR 2.[8]

Possible consent models include:[9]

- No consent
- Opt-out
- Opt-out with exceptions
- Opt-in
- Opt-in with restrictions

Opt-out models tend to have increased patient participation because opt-in models require more effort on the part of the patient to provide consent. Opt-in models often include specially protected health information since the patient specifically consents to the information exchange. Patients should be able to decide how their electronic health information is exchanged. This decision could be made through a "meaningful choice," either an opt-in or opt-out model, or a more granular consent as long as they are informed of how and why their information will be exchanged in advance of making the decision to participate.

Release of Information Challenges

Many laws and regulations currently govern how, when, what, and to whom protected health information is released. The Health Insurance Portability and Accountability Act (HIPAA) privacy rule and HITECH Act contain specific requirements for the management of personally identifiable health information that balance confidentiality of the individual with the need for complete and timely exchange of health information. These regulations create a new paradigm where we must adapt the traditional release of information functions.

Complete and timely information is critical to providing the best care possible, and excluding certain information from an exchange in certain cases could negatively impact patient care. The challenge of the current complex medical and legal environment is that clear and concise guidelines for release of information are not always provided, and standards may be put into place before the functionality exists to execute them. For example, in a free text discharge summary, the use of metadata tags to identify protected information is difficult.

Consideration of other federal regulations, such as 42 CFR 2 for drug and alcohol patient records, further complicate the HIE environment. The consent requirement for these records is often perceived as a barrier, but it is important for HIM professionals to understand the details of the regulation and assist in the development of business processes and application requirements.

Varying state regulations require HIEs to assume 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.

HIM professionals can assist HIEs in overall management of the release of information (ROI) process in order to ensure confidentiality, security, and compliance in releasing protected health information. It is crucial for policies and procedures to include guidance on those practices that support oversight of disclosures of information.

HIM Contributions to HIE

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:

- Drafting data governance and stewardship policies, including data ownership, data integrity, and data quality
- 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

---

Meaningful Choice and HIE

The program information notice (PIN), introduced on March 22, 2012 by ONC, outlines privacy and security framework requirements and guidance for establishing robust privacy and security policies and practices for exchanging health information.[10] This provides the common set of privacy and security rules of the road and assures provider and public trust in enabling progress in health information exchange to support patient care.

The individual choice section within the PIN outlines that an individual should be able to designate a family member, caregiver, domestic partner, or legal guardian to make decisions on their behalf. If the HIE stores, assembles, or aggregates information beyond a directed exchange (i.e., provider-to-provider via encrypted e-mail), it should ensure individuals have "meaningful choice" regarding the exchange of information through the HIE. Patient choice is not required if the HIE uses directed exchange and does not access or use the information.

Meaningful choice signifies:

- Choice is made with advance knowledge/time
- Not used for discriminatory purposes or as a condition for receiving medical treatment
- Choice is made with full transparency and education
- Commensurate with circumstances for why individually identifiable health information (IIHI) is exchanged
- Consistent with patient expectations
- Revocable at any time

Healthcare providers will be challenged to provide patients in advance with meaningful choice, and they have several options as to the method of provision, such as paper brochures or flyers, consents, and online patient portals. Ensuring patients are provided meaningful choice will require education and awareness.

Conduct Careful HIE Vendor Selection

A thorough vendor selection process should include a detailed request for proposal (RFP) that outlines the HIE's key requirements-including the technical requirements of the system and privacy and security requirements.

The technical requirements may include such things as compatibility with Direct, CONNECT, record locator services, and master patient indexes. The technical requirements should be based upon the strategic and operational plan developed by the state HIE designated entity and approved by ONC.

As a starting point for vetting privacy and security requirements, the RFP should require the vendor to address functionality based upon the fair information practices:

1. Individual access
2. Correction
3. Openness and transparency
4. Individual choice
5. Collection, use, and disclosure limitations
6. Data quality and integrity
7. Safeguards
8. Accountability

For example, under the section "Individual Choice," there are opt-in/opt-out models. The vendor should address if and how their system can facilitate each option. Additionally, they should identify how granular the system can get with their consent module. Can they limit specific information, such as an HIV test, or is the module limited to an "all-in" or "all-out" functionality? If it is the latter, the vendor should identify when and if they plan to add this functionality.

To ensure that the system has the necessary components to handle ROIs in accordance with HIPAA, HIM professionals must be involved in the development of the RFP and the vendor selection. Since each HIE is unique, no two HIEs will act or exchange information in the same manner and each may have different system requirements.

HIM's HIE Responsibilities Defined

The HIM profession is changing each day. 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 are assuming leadership roles within HIE organizations providing testimony, volunteering on HIE committees, and securing key leadership roles at the workgroup, staff, 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.

Patient Identification Management

Accurate patient identification and successful linking of electronic records is highly dependent on the accuracy of key demographic data. There are three different events that must occur in order to maintain patient identity data integrity:

- The data must be collected correctly
- The data must be entered correctly
- The data must be queried correctly

Errors during any of these three events create opportunities for inaccurate patient identity. As the organization becomes larger, the volume of these events grows and there is a proportionately increased opportunity for patient identity errors. These errors

become compounded when an organization becomes part of a larger network or incorporates other entities' information into its own.

The underlying causes of identity errors are numerous. Some causes include people and process issues such as registration and scheduling staff selecting the wrong patient (causing an overlaid record) or the registrars entering the data to be searched incorrectly (causing either an overlay or a duplicate). Other identity errors are caused by technology challenges such as loose algorithmic record matching that causes incorrect electronic linking or auto-merging of records, or ineffective record search algorithms that prevent a registrar from finding the patient's previous record.

Another common cause is data stored in the enterprise master patient index that is not current for the patient (i.e., last name change) and the searched data is different from the data stored in the system-resulting in a duplicate record. Related to this data integrity challenge, records in the historical database often have inadequate identifying information about the patient, causing the registrar to have to create yet another record for the patient-and therefore a duplicate. Many other data integrity scenarios exist, and combinations of all of these scenarios create even more complexity. As databases get larger, the complexity of the data integrity grows exponentially.

The HIM challenge is managing multitudes of detailed data on thousands of records and millions of transactions each and every year. A strong data quality and control program must be maintained or the data will get out of control quickly in a health information exchange environment.

The State of HIE in 2011

A 2011 report from the eHealth Initiative found that 2011 brought significant change in the health information exchange environment.[11]

- The number of HIE organizations continues to grow, with a total of 255 HIE initiatives in 2011, up from 234 in 2010.
- Out of the 196 HIE initiatives responding to the eHealth Initiative's survey, only 24 (12 percent) currently reported being self-sustaining.
- There are 10 initiatives that ceased operating between 2010 and 2011. Four closed down operations, four others consolidated with other HIE initiatives, and two for-profit organizations were purchased and had HIE operations shuttered.
- Defining value, addressing organization and governance issues, privacy and confidentiality issues, and technical aspects of HIE remain top challenges for sustainable HIEs.
- Of the 24 sustainable HIEs, 13 indicated that they will participate in an accountable care organization (ACO), and one indicated they would not participate. Ten initiatives are unsure of their plans regarding ACOs.
- HIEs generally fall into one of three architecture models. Sustainable initiatives utilize all three of these models, but the predominant model is a hybrid architecture.

  - Centralized-characterized by health information and data that resides in one central location
  - Federated-health information is stored at the local or regional level with the HIE services acting as a conduit for exchange between other entities
  - Hybrid-a combination of centralized and federated, often a central repository of information with "edge servers" utilized for data storage

- Sustainable initiatives tend to focus on care coordination services, rather than services that support administrative functions, such as claims and eligibility information.
- Opt-out was the predominant type of privacy model used by sustainable HIEs in 2011, but many initiatives are providing more granular consent at the encounter or data level.

Privacy, Security, and Audits

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.

The lack of a clear and consistent HIE approach to privacy and security may hinder US ability to realize the benefits of electronic HIE. 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
- Accountability

ONC initiated the Strategic Health IT Advanced Research Projects (SHARP) in late 2009 as an American Recovery and Reinvestment Act initiative.[12] This initiative provides funding for research that focuses on addressing problems that have impeded providers' ability to adopt and meaningfully use health IT. The program itself is led by collaborative efforts at the University of Illinois at Urbana-Champaign, the University of Texas at Houston, Harvard University, the Mayo Clinic of Medicine, and Massachusetts General Hospital. Research is currently being conducted in several areas, including security of health information technology.

The University of Illinois at Urbana-Champaign is helping to develop technologies and policy recommendations that reduce privacy and security risks and increase public trust. This research encompasses three projects: EHRs within a single healthcare delivery organization, telemedicine, and HIE. The HIE project is concerned with security and privacy of health records as they are exchanged between care delivery organizations or individuals. The **Secure Health Information Exchange project** addresses the inadequacy of current exchange service models. The **Experienced-based Access Management project** limits insider threats through a continuously evolving model for access control rules. And the **Personal Health Records project** address third-party personal health record (PHR) privacy standards with PHR stakeholders.

HIM professionals have a responsibility to maintain a keen awareness of the developing HIE environment so they can develop, implement, and update systemwide 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 it.

ARRA Spurs HIE Development

ARRA-authorized incentive programs under the Centers for Medicare and Medicaid Services began to pay bonuses to "meaningful users" of certified EHRs beginning in fiscal year (FY) 2011, but will phase in penalties for those failing to meet "meaningful use" beginning in FY 2015. To be eligible for the incentives and avoid future payment penalties, hospitals and physicians must use EHRs that have been certified through a federal certification process established by ONC to meet specific meaningful use quality measurement requirements.

The Centers for Medicare and Medicaid Services' stage 2 meaningful use final rule and ONC's standards and certification final rule were published in the Federal Register on September 6, 2012.[13,14] Taken together, these regulations raise the bar on EHR adoption requirements that hospitals and physicians must meet under ARRA to continue to qualify for additional Medicare and Medicaid incentive payments, as well as to avoid significant payment penalties starting in 2015.

The EHR Incentive Program has dramatically increased the number of HIEs throughout the US. In stage 1 of the program, providers must show that their EHR systems could exchange health information. The final rule for stage 2 involves higher expectations for HIEs, such as tougher requirements for e-prescribing, structured laboratory results, and expectations that providers will electronically transmit patient care summaries to support care transitions. The increasingly robust expectations for health information exchange expected in stage 3 will support the overall goal of having information follow the patient.

The lack of standards has created challenges for connecting HIEs. In addition to state and federal rules and regulations imposed on HIE systems, industry and vendor standards may vary, making it nearly impossible for HIEs to connect within the same local area-much less across states. The currently optional standards for HIEs greatly reduces the ability to share patient information when needed.

Stage 2 sends us down a path of having more consistent standards and operational processes to support this work. Additional information on the Medicare and Medicaid EHR Incentive Programs can be found at www.cms.gov/EHRIncentivePrograms.

Appendices

The following three appendices are available in the online version of this practice brief only.

Appendix A: Volunteer Position Description for CSA Health Information Exchange Representatives

Date: 08/22/12
Reports to: CSA Board of Directors

Position Summary:

The Component State Association (CSA) representative for the health information exchange (HIE) serves to guide the HIE's efforts utilizing sound HIM principles that include protective measures that support the privacy and security of health information and provide a foundation to ensure health information integrity.

Responsibilities:

- Represent the CSA in the development of HIE initiatives and adoption of health information technologies to effectively support health information exchange.
- Serve in a consultative capacity when interacting with potential subscribers and members of the exchange network to derive effective policies in the areas of personal health records and exchange of information among authorized entities, providers, and health systems.
- Provide professional guidance in the development of policies and procedures for privacy and security of health information and maintaining its integrity.
- Participate in describing and defining data integrity rules, including but not limited to describing typical records, data, and document types that could be exchanged.
- Identify long-term opportunities to effectively model and use de-identified health information to promote public health initiatives and result in safer, higher quality, and more efficient delivery of healthcare.
- Serve as a resource for current efforts by health information technology and HIE standard development groups (i.e., HL7, ASTM, ONC, etc.).
- Collaborate with HIEs within the state to advocate for national policies that make sense for the HIM profession and support efficient, practical provision of healthcare treatment and business operations that results in quality data being used to improve patient care.
- Contribute to official HIE comments and responses to Congress, the state legislature, and federal and state agencies concerning technical standards that affect HIEs, EHRs, PHRs, and the development of the national health information network.
- Support the infrastructure design for evaluating and monitoring system security, privacy, and business continuity back-up systems.
- Guide HIE organization colleagues on practice variances across care settings.
- Educate colleagues and lead the challenge to ensure patient identity management and master person index (MPI) integrity-including developing system rules to ensure data integrity, managing MPI design, and ensuring maintenance and ongoing operations such as defining record location services.
- Contribute to policy development for HIE entities, including authentication, privacy, security, auditing, patient matching, opt-in/opt-out, complaint, and consent.
- Provide guidance on establishing an HIE governance mechanism. Aid in grant writing.
- Serve as a liaison with the HIE legal, IT, and workgroup on appropriate policy issues.
- Represent the CSA and HIM profession by attending technical meetings with the goal of guiding the scope of work in accordance with best practices for HIM, privacy, and security.
- Develop educational tools to be used to explain the HIE and use of its system for the participants of the HIE network.
- Develop educational materials to inform the CSA constituents and public of the HIE activities.

- Provide community education about HIEs (in general), EHRs, and PHRs as a public service and outreach.

Desired Qualifications:

- Commitment to working in a team environment with an ongoing emphasis on partnering and sharing work with colleagues
- Exemplary interpersonal skills that translate into positive relationships with colleagues
- Solid communication skills including the ability to concisely explain complicated concepts to executives and leaders within and outside of the HIE both in oral and written form
- Project management skills
- Ability to establish credibility and be viewed as a strategic health information expert
- HIE expertise and knowledge, particularly related to the role of health IT and HIE in improving quality
- An understanding of health information system interfaces, including test-specific modules (i.e., laboratory, radiology, etc.) and controlled medical vocabularies
- A solid understanding of enterprise MPI and record locator service development
- Experience with a combination of clinical, health information, and information systems
- Knowledge of networking, health information exchange, and messaging and document standards
- Knowledge of HITSP component and base standards, the Nationwide Health Information Network, Direct Project, CONNECT Open Source Solution, and health information privacy and security regulations

Developed by the HIE Practice Council-Privacy and Security Mission Critical Team 2009.

Reference:

AHIMA. "[Understanding the HIE Landscape. Appendix B: Volunteer Position Description for CSA Health Information Exchange Representatives](#)." *Journal of AHIMA* 81, no.9 (September 2010).

Appendix B: Talking Points for HIM Professionals

HIM professionals are uniquely qualified to participate in HIE development and operations. However, those involved with developing and running many HIEs often do not realize the value that HIM professionals bring to the table.

If HIM professionals are not involved in your local HIE, reach out to the HIE and ask for the opportunity to meet with them. When meeting with HIE staff, convey who AHIMA is, the HIM professional knowledge and skill set, and how HIM professionals can assist in developing and implementing information management practices. Relate how each of these values allows HIM professionals to contribute to the structure, governance, and operations models of the HIE. The following talking points may assist CSA leadership and HIM professionals in discussing information exchange and management.

AHIMA Facts: AHIMA is the premier association of HIM professionals. AHIMA's more than 64,000 members are dedicated to the effective management of personal health information required to deliver quality healthcare to the public. Founded in 1928 to improve the quality of medical records, AHIMA is committed to advancing the HIM profession in an increasingly electronic and global environment through leadership in advocacy, education, certification, and lifelong learning.

Quality Healthcare through Quality Information: Quality information is essential to all aspects of today's healthcare system. HIM is the body of knowledge and practice that ensures the availability of health information to facilitate real-time healthcare delivery and critical health-related decision making for multiple purposes across diverse organizations, settings, and disciplines.

Leader in the Management of Health Information: Founded in 1928 to improve health record quality, AHIMA has played a leadership role in the effective management of health data and medical records needed to deliver quality to the public. Historically, medical records have been a paper-based business. However, with the advent of e-HIM practices, HIM professionals are working to advance the implementation of electronic health records by participating and leading industry

initiatives such as HIPAA privacy and security rule implementation efforts, e-MPI management, and developing the future workforce. HIM skills and knowledge are transferrable from paper to electronic practices.

Partner in the Delivery of Quality Healthcare: HIM professionals work in 40 different settings under 125 different job titles. They often serve in bridge roles, connecting clinical, operational, and administrative functions. In short, they affect the quality of patient information and patient care at every touchpoint in the healthcare delivery cycle. Having skilled HIM professionals on staff ensures an organization, or HIE, has the right information when and where it is needed while maintaining the highest standards of data integrity, confidentiality, and security.

Advocate for Healthcare Policy: With national focus on health information, EHRs, ARRA, HITECH, and information exchange across the country, AHIMA is qualified to shape the national agenda. Change is happening on four fronts:

- Privacy and security
- Standards for data interchange and system interoperability
- The EHR
- The overall national health information infrastructure

With HIM's overriding goal in mind-ensuring the availability of health information to facilitate real-time healthcare delivery-AHIMA is involved in initiatives advancing the role of HIM in informing clinical practice, developing standards to improve data quality and facilitate information exchange, and helping healthcare organizations migrate to the EHR.

Valuable Professional Resources: AHIMA keeps HIM professionals posted on the healthcare industry through multiple resources. The award-winning *Journal of AHIMA* delivers news and expert guidance. AHIMA textbooks are recognized for their excellence and authority. Members can also receive electronic newsletters that deliver up-to-the-minute industry updates and advice.

Questions to Ask:

1. What vendor has the HIE chosen? If no vendor has been chosen, provide a copy of AHIMA's RFP practice brief, "The RFP Process for EHR Systems."
2. Will state Medicaid (or other federal payers such as prisoners, workers' compensation, Indian Health Services, or veterans) recipients be automatically enrolled in the HIE?
3. Will the HIE sign a business associate agreement (BAA) with each covered entity? Does the BAA address how breaches will be handled? Is the BAA compliant with state-specific notification requirements? Provide the HIE with copies of AHIMA's HITECH-revised BAA.
4. How will the HIE address patient identity management? Provide the HIE with a copy of AHIMA's practice brief "Reconciling and Managing EMPIs."
5. How will the HIE address release of information functions? Provide the HIE with a copy of AHIMA's practice brief "Management Practices for the Release of Information."
6. Will the HIE have a structured HIM department?
7. What types of tools and resources will the HIE provide to patients to assist in managing the bidirectional exchange of information?
8. What is the governance structure of the HIE? Is the HIE opt in/opt out?
9. Does the HIE have an HIM professional representative either on the board, subcommittee, or workgroup?
10. Who will have access to the data and under what conditions (i.e., law enforcement, attorneys)?
11. What specific data elements will be shared by each participant?
12. Does the HIE have specific standards or formatting requirements for the data or other technical requirements (i.e., HL7 sending and receiving formats)?
13. Will participants have the option to audit the HIE for privacy and security reasons?
14. How will the HIE address requests for restrictions, accounting of disclosures, and other privacy issues?
15. What is the process for a participant who withdraws or terminates data sharing with the HIE? Can a participant be expelled from the HIE?
16. Are there any associated fees required for participation?
17. Who will provide training and support to consumers?
18. Is there a comprehensive list of responsibilities that includes individual responsibilities of the HIE, organization, and provider?
19. How will the HIE address accounting of disclosures and data breaches?

HIM professionals should provide the HIE with the link to AHIMA's HIE (http://www.ahima.org/resources/hie.aspx [web page no longer available]) and ARRA (http://www.ahima.org/advocacy/arrahitech.aspx [web page no longer available]) web pages.

Reference: AHIMA. "[Understanding the HIE Landscape. Appendix C: Talking Points for HIM Professionals](#)." *Journal of AHIMA* 81, no.9 (September 2010).

Appendix C: Data Governance Policies Purpose Statements

Date: 08/22/12

The following is a list of recommended data governance policies that health organizations should develop and implement. This list is not meant to be all-inclusive.

1. **Data Conversion Planning Policy:** To prevent post-conversion workflow issues, data quality problems, patient safety issues, and inefficiencies in any or all departments. Achieving successful Master Person/Patient Index (E/MPI) data conversions requires thorough, well-documented plans.
2. **Enterprise Data Integrity Maintenance Policy:** To ensure the data integrity and accuracy of all electronic systems within or integrating with the organization's EHR including hospitals, clinics, diagnostic centers, and other health delivery provider locations and health information exchange organizations.
3. **Policy on an Integrated Medical Record:** To ensure that all providers at the health provider organization, including the hospitals and clinics at all health delivery provider locations, has access to an integrated, complete medical record for all of the organization's patients.
4. **Core Patient Identifiers and Naming Convention Policy:** To ensure each patient of the health provider organization has a complete name captured in each administrative, business, and clinical system and other core patient identification data facilitating the accurate identification of the patient and optimizing electronic record linkage across all of the health provider organization systems.
5. **Medical Record Corrections Policy:** To assure that all administrative, business and clinical systems and all data fields in each system's tables and documents accurately reflect each patient's clinical and demographic data.
6. **Duplicate Record Validity Determination Policy:** To ensure a consistent methodology for determining whether two records truly belong to the same person/patient and that a centralized process for training on duplicate record validity occurs.
7. **Record Search Policy:** To standardize how searches are performed before creating a new person or patient record in the organization's scheduling, registration, or EHR systems.
8. **Data Conversion Testing Policy:** To standardize how data conversion testing for any electronic record system conversion will occur.
9. **Electronic Record Linking Policy:** To ensure all systems that are electronically interfaced utilize a minimum set of criteria for record matching, thereby reducing the opportunity for overlaying an existing medical record with another patient's information and assuring accurate record matching between all electronic systems.
10. **Maintenance of User and Provider Master Records Policy:** To ensure all users of electronic systems at the health organization have proper authentication, have adequate data to verify the identity of each user, and that the user records are properly maintained.
11. **Patient Involvement in Medical Record Accuracy Policy:** To provide a mechanism for the health organization's patients to request and validate corrections to their medical record, thereby optimizing the quality, accuracy, and integrity of the content of the organization's medical records.
12. **Legal Medical Record and eDiscovery:** Defines what the organization's legal health record includes and the processes and technology in place that support eDiscovery.
13. **Data Ownership and DURSA Agreements:** To provide guidance on who owns patient-identified health information, who owns aggregated de-identified data, and what principles should be used to determine how de-identified patient health information (data) may be used.
14. **HIE Opt in/Opt Out:** To define the organization's patient education and staff processes when implementing the HIE Opt in/Opt out policy.
15. **Red Flag Alert:** To identify the alert mechanisms in place to detect potential medical identity fraud or theft and the communication process in place to follow up on the red flag investigation.

16. **Data Governance Terms and Definitions:** To ensure clear, complete, and unambiguous communication across all data governance policies of common terms utilized in each policy.

Developed by the HIE Practice Council 2012.

Notes

1. KLAS Research. "Health Information Exchanges: Rapid Growth in an Evolving Market." 2011. https://www.klasresearch.com/Store/ReportDetail.aspx?ProductID=642.
2. HHS. "Nationwide Health Information Network: Conditions for Trusted Exchange." *Federal Register*. May 15, 2012. http://www.gpo.gov/fdsys/pkg/FR-2012-05-15/pdf/2012-11775.pdf.
3. HHS. "Privacy and Security Tiger Team." The Office of the National Coordinator for Health IT. June 6, 2012. http://healthit.hhs.gov/portal/server.pt/community/healthit.hhs.gov:_privacy_&_security_tiger_team/2833/home/19421.
4. Federal Trade Commission. "Fair Information Practice Principles." November 2012. http://www.ftc.gov/reports/privacy3/fairinfo.shtm.
5. HHS. "About CONNECT." CONNECT Community Portal. http://www.connectopensource.org/.
6. HHS. "NHIN Architecture Overview." DRAFT v0.9 April 21, 2010. http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_11113_911643_0_0_18/NHIN_Architecture_Overview_Draft_20100421.pdf.
7. American Recovery and Reinvestment Act of 2009. Section A, Title XIII, Health Information Technology. http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/hitechact.pdf.
8. Electronic Code of Federal Regulations. Code of Public Health. Title 42. Part 2-Confidentiality of Alcohol and Drug Abuse Patient Records. http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&rgn=div5&view=text&node=42:1.0.1.1.2&idno=42.
9. NGA Center for Best Practices. "State and Federal Consent Laws Affecting Interstate Health Information Exchange." March 2011.
10. ONC. "The Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information." March 11, 2010. http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__privacy___security_framework/1173.
11. eHealth Initiative. "2011 Report on Health Information Exchange: Sustainable HIE in a Changing Landscape." 2011. http://www.ehealthinitiative.org.
12. ONC. "Strategic Health IT Advanced Research Projects (SHARP) Program." April, 28, 2011. http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__sharp_program/1806.
13. HHS. "Medicare and Medicaid Programs; Electronic Health Record Incentive Program-Stage 2." *Federal Register*. September 4, 2012. http://www.gpo.gov/fdsys/pkg/FR-2012-09-04/pdf/2012-21050.pdf.
14. HHS. "Health Information Technology: Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology, 2014 Edition; Revisions to the Permanent Certification Program for Health Information Technology." September 4, 2012. http://www.gpo.gov/fdsys/pkg/FR-2012-09-04/pdf/2012-20982.pdf.

References

ONC. "State Health Information Exchange Cooperative Agreement Program." August 11, 2012. http://healthit.hhs.gov/portal/server.pt?open=512&objID=1488&parentname=CommunityPage&parentid=58&mode=2&in_hi_userid=11113&cached=true.

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

Prepared By

Kathy M. Callan, RHIA
Beth H. Just, RHIA, FAHIMA
Annessa Kirby
Jackie Raymond, RHIA
Harry Rhodes, MBA, RHIA, CHPS, CPHIMS, FAHIMA

Kathy J. Westhafer, RHIA, CHPS
Sheldon Wolf

Acknowledgements

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* 84, no.1 (January 2013): 56-63.

Driving the Power of Knowledge