

HIM Principles in Health Information Exchange

Emerging health information exchange initiatives must focus on more than their IT model. They must make important early decisions on HIM issues that hard-wire data quality, privacy, and security into the network, ensuring that the ultimate goals of improved patient safety and quality of care are met.

The value of electronic healthcare data exchange was demonstrated in the aftermath of Hurricane Katrina, when healthcare organizations throughout the region and nationwide shared patient data to aid in the care of residents displaced by the storm.

The Department of Veterans Affairs found that more than 2,300 users exchanged electronic healthcare data across 48 states in the month following the disaster. Laboratory data represented just 2 percent of all data requests. Text-based reports including demographics, discharge diagnoses, immunizations, and health summaries were the most commonly requested reports.¹

Technology is a critical tool in achieving the benefits of health information exchange (HIE). However, technology alone is not sufficient. Healthcare industry stakeholders that base their HIE solutions solely on technology do so at the expense of underlying HIM principles. An abundance of disparate HIE principles, models, definitions, products, and standards camouflages some crucial policy and process decisions an HIE initiative must make in the early stages of its development.

Transmitting patient data electronically without attending to the business processes surrounding data capture, translation, and transmission has the potential to increase patient risks and healthcare costs. Data accessibility, reliability, and accuracy are critical factors in obtaining the trust of stakeholders, including consumers, and in sustaining long-term data exchange on a large scale. Accordingly, it is imperative for regional health information organizations (RHIOs) to hard-wire patient safety and quality of care measures into the HIE's processes and systems.

This practice brief outlines the HIM principles essential to HIE initiatives. The manner in which HIM principles apply to an HIE are discussed further in the "Data Quality Attributes Grid," available in the online version of this practice brief in the FORE Library: HIM Body of Knowledge at www.ahima.org. The "Data Quality Management Model," also available in the online version, describes key process issues that are important to the success of an HIE.

Establishing Standards in HIE

There has been continued progress in the development of EHR standards, including electronic transmission methods for HIEs and the nationwide health information network. AHIMA is now calling for the development and implementation of HIE standards for the quality of data content, data mapping, and clinical documentation. These standard HIM

principles can ensure the accurate transmission of data across participating RHIOs.

A commitment to core HIM principles is as important in the electronic health information environment as it is in the paper realm. HIM professionals must convert their critical principles to the electronic environment and effectively build such principles into HIE workflows. As RHIOs form, HIM professionals must help these organizations:

- ▶ Define the data exchange model and the specific data to be exchanged based on the RHIO's mission, vision, purpose, and goals
- ▶ Develop standards for acceptable data quality that will be required of RHIO participants, as well as how data quality will be measured
- ▶ Assess the process to capture patient identity as well as its consistency across each of the RHIO's participating organizations
- ▶ Provide standards for each RHIO participant's duplicate medical record rate and outline how this rate will be measured to ensure validity
- ▶ Audit the accuracy of the electronic linking of records within the RHIO and provide evidence of the accuracy rate
- ▶ Audit the accuracy of the clinical documentation within RHIO participants' electronic medical record and report the results to the RHIO's governing board
- ▶ Develop privacy and security policies regarding methods for accessing the RHIO system, provisioning, authorizing, and authenticating users, and auditing access

Defining RHIOs

A RHIO is a group of organizations and stakeholders that exchanges data electronically to improve the quality, safety, and efficiency of healthcare delivery.² RHIOs are ordinarily geographically defined entities that arrange for the means to exchange information electronically. They also develop and maintain HIE standards. To successfully exchange information, RHIOs must build their data exchange on sound principles and processes.

With significant federal and private investments in RHIOs, new projects are being formed continuously, each with varying purposes and objectives. The purpose drives the method by which a RHIO shares electronic clinical information. The various clinical data-sharing models, in turn, require different privacy and security policies and data controls.

RHIO Building Blocks

A RHIO's purpose drives the method by which it shares electronic clinical information. Various clinical data-sharing models, in turn, require different privacy and security policies and data controls.

Upon its initial formation and the establishment of its governance structure, a RHIO needs to clearly define its purpose and its clinical data-sharing needs. This sound foundation forms the basis for the operational, process, and technology building blocks that follow. This diagram outlines these building blocks, providing a high-level overview of the timing and general flow of key phases and steps that should occur early in a RHIO's development. RHIOs must establish sound HIM data exchange principles in order to ensure the quality of data shared and optimize the quality of care delivered.

Assess performance improvements created by HIE ("value"):
<ul style="list-style-type: none"> Quality improvement Cost improvement Patient care access improvement
Assess RHIO sustainability
Perform security and downtime audits
Monitor system performance, load balancing
Manage data integration failures, duplicates, overlaid records
Report to HIE participants on data integrity issues:
<ul style="list-style-type: none"> Overlaid records Duplicate records Invalid data sent
Complete stakeholder consumer education
Monitor report and audit trails
Apply corrections – interfaces

Stage 4—Evaluation

Once live, the RHIO must measure its performance against its goals and assess the value it delivers. Just as important as its ability to provide value is the RHIO's ability to sustain itself over time.

Stage 3—Implementation

As the RHIO moves from its design stage, it plans the system implementation and the business process requirements. Data sharing, data ownership, data stewardship, access and authentication, and privacy and security policies should be finalized. This stage ends with go-live.

Go live	3. Follow-on training
	2. Production testing (functional, regression, integration)
	1. Audit trail monitoring (authentication, access, breach assessment)
Implement policies and procedures	
Implement system	6. Data integration and linking evaluation
	5. Test (unit, functional, regression, integration, audit logs, reports)
	4. Training
	3. Build
	2. Develop privacy, security, and data retention policies and procedures
	1. Design
Design patient opt-in/opt-out methodology	
Develop detailed project plan	6. Design user access, authorization, and administration
	5. Interface design
	4. Application build
	3. System design and build
	2. Network configuration
	1. Staffing selection (design, build, support, training, data maintenance)

Stage 2—Design

Building on the decisions in the formation stage, the RHIO next identifies the types of data participants will exchange and establishes how that data will be shared. These decisions drive selection of the technology.

Develop reporting timing and methodology to HIE participant (contributor sources)	
Select technology solution	
Develop RFI or RFP	
Research and understand differences between CCHIT certifications	
Develop detail functional and system requirements	4. Scope clinical data to be exchanged, both long term and short term
	3. Determine reporting requirements
	2. Define patient demographic data to be stored (if applicable)
	1. Architecture design and network topology
Analyze contributor sources and systems to HIE	2. Perform gap analysis across sources
	1. Determine data sources

Stage 1—Formation

In the first stage, the RHIO defines its purpose and prepares plans to clarify needed participants, governance, data-sharing requirements, compliance, and other key strategic issues.

Develop participant compliance, educational, communication plans	
Determine critical path for solution design and implementation	
Develop community support plan	
Decide on clinical data-sharing model	
Develop privacy, security, and data ownership and stewardship policy guidelines	
Prepare strategic plan	5. Technical model
	4. Access and authentication model
	3. Clinical data-sharing model
	2. Business model (initial funding sources, ongoing funding sources, return on investment analysis, organizational structure)
	1. Government model and legal entity
Clarify stakeholder understanding of clinical data-sharing models and privacy and security laws and regulations	
Inventory executive support from needed organizations (such as providers)	
Prepare high-level project plan	
Define RHIO's mission, vision, purpose	
Identify key stakeholders (individuals, organizations, champions): consumers, employers, health plans, health department/public health, law enforcement, first responders, nursing homes, clinics, utility companies, epidemiology, medical researchers, and others	

Upon its initial formation and the establishment of its governance structure, a RHIO needs to clearly define its purpose and its clinical data-sharing needs. These key decisions will direct the remaining operational, process, and technology building blocks. The diagram on the preceding page outlines these building blocks, providing a high-level overview of the timing and general flow of key phases and steps that should occur early in a RHIO's development. RHIOs must establish sound HIM data exchange principles to ensure the quality of data shared and optimize the quality of care delivered.

The "RHIO Checklist," available in the online version of this practice brief, shows the development and implementation stages as well as HIM involvement in the process. The checklist also provides definitions for the RHIO building blocks diagram and directs the reader to additional documents and references.

Clinical Data Exchange Models

Health information exchange is the actual electronic mobilization or movement of healthcare information across organizations within a region or community. HIE is the capability to move clinical information electronically between disparate healthcare information systems while maintaining the accuracy of the information being exchanged. Its goal is to facilitate access to and retrieval of clinical data to provide safer, more timely, efficient, effective, and patient-centered care. The term does not define the governance of the exchange model or the purpose of the information exchange.

The Healthcare Information and Management Systems Society outlines three different clinical data exchange models: federated, centralized, and hybrid.³ Numerous and broad variations of these architectures currently exist. These architectures also are used in combination to achieve clinical data exchange. For instance, public health agencies may use a clinical data exchange model that employs both the federated and centralized data exchange architectures, using an immunization database to store immunization-related data centrally in one database, but using a federated mechanism to link data about one patient reported from various providers.

A second hybrid architecture example is a statewide RHIO that uses a centralized database to create a record locator service (RLS) to link patient records across the various participant databases. In this model, a peer-to-peer network is established, allowing each participating organization the ability to authenticate its users. Participating organizations maintain their own clinical databases or repositories.

The RHIO then builds a communication portal between RHIO participants, local clinical databases, and the RLS. The authorized user can search the RLS, find and select the patient, and cue the communication application to generate a real-time message to all participating clinical databases that contain clinical data for that patient. The clinical databases

receive the request message and send back all appropriate clinical data to the requestor in real time.

Several of these models as well as examples of currently operating models are described in more detail in "Clinical Data Exchange Models," available in the online copy of this practice brief. The document also addresses the advantages and disadvantages of various clinical data-sharing models and notes which models might be selected by a RHIO based on its mission, vision, purpose, and goals.

Issues and Obstacles

To date, healthcare organizations planning for HIE are not fully considering key HIM principles and functions during the formation and design phases. The common focus is on the technical exchange of data between systems, not on ensuring the quality of the data exchanged. HIM professionals on these teams must facilitate focused and comprehensive conversations about data validity and integrity and the quality of key data values. Questions to ask include:

- ▶ How have other RHIOs developed policies and procedures that ensure data quality attributes?
- ▶ What is the contamination rate of MPI systems?
- ▶ What is the RHIO's defined purpose and mission for exchanging health information as it relates to patient safety and quality patient care?
- ▶ How will the RHIO hold participants accountable for the accuracy of the clinical documentation and results shared among participants?

The online appendix "Use Case Scenarios," shows how easily inaccurate data can be sent between systems. History has shown that the success of an EHR implementation correlates directly with data trust, confidence level, and use. The success of data exchange projects will be no different.

When stakeholder EHR systems are later interfaced to RHIOs, the clean-up work will be labor intensive. Who will ensure accurate patient identification can be achieved on the front end, at the point patient identity data are captured? The accurate patient identity section in the "Use Case Scenarios" provides an illustration of this challenging piece to the HIE puzzle.

The RHIO building blocks should occur in the sequence presented in the diagram on page 70. Additionally, the following critical issues must be discussed early in a RHIO formation to minimize the occurrence of common obstacles:

Understand what clinical data will be exchanged (see the "RHIO Checklist" and "Clinical Data Exchange Models" online). Address this decision early in development, shortly after the governance phase. The decision should be based on the mission, vision, purpose, and goals of the RHIO and must occur long before any discussions of technology solutions.

Define process and technology requirements based on the clinical data exchange. This should lead to selecting

the clinical data exchange model, which, in turn, will help define what data actually will be stored by the RHIO (e.g., will only RLS-level data be stored, or will clinical data also be stored?).

Define what PHI will not be shared and what information requires special protection under applicable laws prior to disclosing any information to or through the RHIO. This also helps in understanding how clinical data will be requested and received by the participating providers. Questions developing RHIOs must ask include:

- ▶ Will the requestor have to make a separate request for information directly to the participating organization that stores that clinical data? If so, how will this request occur?
- ▶ How will the participating organization respond to the request (via fax, secure e-mail, etc.)?
- ▶ If electronically facilitated by the RHIO, will the clinical data be “pushed” to all providers linked to the patient, or will the requestor complete an electronic request that results in the clinical data being “pulled” from the participating organization’s EHR by the requestor?

Before a system can be selected and implemented, these questions must be answered in order to specify the requirements of the system.

Develop privacy and security policy requirements and the provider authorization and authentication requirements as determined by the clinical data exchange model. These requirements can only be developed after the above items are addressed (for more information, read the November–December 2006 practice brief “Privacy and Security in Health Information Exchange”). The security of stored patient data (or of the network providing user access) is another significant challenge in HIE. Organizations must ask themselves:

- ▶ How will users be authorized and authenticated?
- ▶ Who controls the authorization and authentication?
- ▶ How is one provider user mapped from one participating organization to another participating organization?

RHIOs must define how users are added, removed, and sanctioned for data access violations.

Decide how patient records are linked when records come from a variety of participating organizations. This is a significant challenge requiring answers to the following questions:

- ▶ What patient identity data will be defined and used to connect patient records across the various participating organizations?
- ▶ What record-linking algorithms will be used?
- ▶ How are these algorithms tested and validated?
- ▶ How will the RHIO resolve duplicates that originate within one participating organization (not overlaps

across participating organizations)?

- ▶ What duplicate record standards will participating organizations be held to, and how will this be measured?

Clearly define data ownership and data stewardship and reflect it in policies for data access, use, and control. RHIOs must determine the gold standard of each data source and agree who owns the data, including duplicate record tables and data transaction logs. RHIOs must define the data they “own” and their information stewardship responsibilities. Questions related to data ownership and stewardship, as well as the accuracy of the record linking and the actual clinical data shared, include:

- ▶ How can information be deleted from the RHIO?
- ▶ How long will information be stored in the RHIO database?
- ▶ What happens to patient information if the RHIO closes?
- ▶ What are the data-sharing agreements between the RHIO participants?
- ▶ Who maintains disclosure logs?
- ▶ Will the RHIO be accountable for the accuracy of the clinical data submitted or provided by each of its participating organizations?
- ▶ What data stewardship issues must be addressed?
- ▶ What are the data quality standards, and how will these standards be defined?
- ▶ What are the data quality metrics participating organizations must meet? What happens if they don’t?

Develop and manage a data quality assurance program.

A data quality assurance program’s mission is threefold: improve data integrity, prevent or minimize errors, and monitor ongoing data integrity. The program’s goal is to attain high levels of data integrity for which the organization is responsible. It must encompass all existing critical databases and, more importantly, be a part of every project that creates new data or that migrates, replicates, or integrates existing data. It must address not only the accuracy of data when initially collected, but also accuracy decay, data completeness, data translation, accurate access, and accurate interpretation of the data for users.

Determine the patient’s role in accessing or updating data stored by the RHIO. Questions to answer include:

- ▶ How will patients be notified about the RHIO?
- ▶ What if patients want to opt out of the RHIO?
- ▶ What role will patients play in ensuring the accurate identification of their records and the clinical data accuracy of the information contained therein?
- ▶ Will patients be able to request restrictions on disclosure of their records in the RHIO?
- ▶ Who will notify patients if there is a privacy breach in the RHIO?

- ▶ If the RHIO provides data that are used for biosurveillance purposes, how does it ensure the accuracy of the data reported?

The personal health record section of the “Use Case Scenarios” provides an explanation of what can occur regarding patients’ involvement in the management of their data. The public health disease surveillance section also provides an example of how data originated by providers may be transmitted to a RHIO or public health database.

Use Case Scenarios

Use case scenarios are often created to illustrate and describe an interaction between a user and a system. The “Use Case Scenarios” appendix, available in the online version of this practice brief, offers a greater understanding of four RHIO issues:

- ▶ The importance of accurate patient identification
- ▶ The patient’s possible role in patient identity or clinical data accuracy
- ▶ How clinical data are reported to public health agencies and used for biosurveillance
- ▶ The critical nature of the accuracy of each piece of clinical data

Conclusion

Ultimately, the goal of RHIOs is to enhance the quality and safety of patient care to benefit patients and the health-care system overall. This can be done by providing greater access to patient information, specifically by ensuring data availability at the point of care. A network of trust is an essential prerequisite for exchange of protected health information, whether that exchange occurs through a community-based information exchange in hospitals and clinics or through a personal health record application.

Although the industry must act within the framework of federal and state laws and regulations, there are ambiguities in these laws and regulations. HIM professionals must play a key role in mitigating these ambiguities by creating policies, processes, and agreements that will satisfy all requirements.

This overview of the HIE process is intended to encourage and assist HIM professionals in participating in data exchange projects. Healthcare workflow, patient rights regarding protected health information, state and federal disclosure laws, secondary uses of protected health information, and data integrity issues including duplicate patient records are all part of the HIM professional’s body of knowledge. This knowledge base uniquely positions the HIM professional to navigate the barriers to RHIO formation and facilitate the definition of key workflows and processes. It also qualifies the HIM professional to assume a leadership role in an HIE project.

The development of widespread HIE is quickly becoming a reality. A great deal of emphasis has been placed on the

technology inherent within HIE solutions. However, it is the optimization and transformation of clinical and business processes enabled by the technology that will improve quality of care and patient safety and reduce costs.

HIM professionals have the opportunity and the responsibility to engage with colleagues and other stakeholders in defining pragmatic, functional business processes in the various systems sharing health data. These processes should be predicated on best-practice data quality principles and attributes that result in improved quality of care and patient safety. ❖

Notes

1. Brown, Steven H., Linda F. Fischetti, Gail Graham, et al. “Use of Electronic Health Records in Disaster Response: The Experience of Department of Veterans Affairs after Hurricane Katrina.” *American Journal of Public Health* 97 (Apr. 2007): S136–S141.
2. Healthcare Information and Management Systems Society. “HIMSS RHIO/HIE.” Available online at www.himss.org/ASP/topics_rhio.asp.
3. Ibid.

Resources

- AHIMA e-HIM® Personal Health Record Work Group. “The Role of the Personal Health Record in the EHR.” *Journal of AHIMA* 76, no. 7 (July–Aug. 2005): 64A–D.
- AHIMA e-HIM Workgroup on Assessing and Improving Healthcare Data Quality in the EHR. “Assessing and Improving EHR Data Quality.” *Journal of AHIMA* 78, no. 3 (Mar. 2007): 69–72.
- AHIMA e-HIM Work Group on Maintaining the Legal EHR. “Update: Maintaining a Legally Sound Health Record—Paper and Electronic.” *Journal of AHIMA* 76, no. 10 (Nov.–Dec. 2005): 64A–L.
- AHIMA Workgroup on Electronic Health Records Management. “The Strategic Importance of Electronic Health Records Management. Appendix A: Issues in Electronic Health Records Management.” *Journal of AHIMA* 75, no. 9 (Oct. 2004): Web extra.
- Avalere Health. “Evolution of State Health Information Exchange: A Study of Vision, Strategy, and Progress.” January 2006. Available online at www.avalerehealth.net/research/docs/State_based_Health_Information_Exchange_Final_Report.pdf.
- Burrington-Brown, Jill, Beth Hjort, and Lydia Washington. “Health Data Access, Use, and Control.” *Journal of AHIMA* 78, no. 5 (May 2007): 63–66.
- Canada Health Infoway. *EHRnews@Infoway* (Winter 2007). Available online at www.infoway-inforoute.ca.
- Carter, Patricia, Chrisann Lemery, Debra Mikels, et al. “Privacy and Security in Health Information Exchange.” *Journal of AHIMA* 77, no. 10 (Nov.–Dec. 2006): 64A–64C.

- dbMotion. "A Practical Approach to RHIO Formation: How an Early Understanding of Technology Can Assist and Accelerate the Process." January 2006. Available online at www.dbmotion.com.
- Health Level Seven. "Electronic Health Record System Functional Model." February 2007. Available online at www.hl7.org.
- Healthcare Information and Management Systems Society. *Guide to Establishing a Regional Health Information Organization*. Chicago, IL: HIMSS, 2007.
- Hirshfield, Marc, and Peggy Daniels Lee. "Critical Success Factors for Healthcare Software Implementations." Available online at www.getvitalized.com/documents/Critical_Success_Factors.pdf.
- First Consulting Group. "Telemedicine in the Ambulatory Setting: Trends, Opportunities and Challenges." March 2007. Available online at www.fcg.com.
- Frisse, Mark. "RHIO Case Studies SW Tennessee." Presentation, eHealth Initiative Summit, March 2005.
- Manatt Health Solutions. "Health Information Exchange Projects: What Hospitals and Health Systems Need to Know." 2006. Available online at www.aha.org/aha/content/2006/pdf/AHARHIOfinal.pdf.
- Office of the National Coordinator for Health Information Technology. "Emergency Responder Electronic Health Record: Detailed Use Case." December 20, 2006. Available online at www.hhs.gov/healthit/documents/AHICEmergencyEHRDetailedUseCase.pdf.

Appendixes

The following appendixes appear in the online version of this practice brief, available in the FORE Library: HIM Body of Knowledge at www.ahima.org:

- › Clinical Data Exchange Models
- › Data Quality Attributes Grid
- › RHIO Checklist
- › Use Case Scenarios

Prepared by

Beth Acker, RHIA
Cassi L. Birnbaum, RHIA, CPHQ
James H. Braden, MBA
Vicki Carlisle, RHIA, CHP
Deresa Claybrook, RHIT
Barbara Demster, MS, RHIA, CHCQM
Stacie Durkin, MBA, RNC, RHIA
Valerie Engel, RHIT
Diane Fabian, MBA, RHIA
Karen Grant, RHIA, CHP
Leah Grebner, MS, RHIA, CCS
Rhonda Hisle, RHIT
Sheri Hutchins, MA, RHIA, CCS
Beth Haenke Just, MBA, RHIA (lead author)
Patricia A. Markus, JD
Rebecca Barron Reynolds, RHIA, MHA
Lorraine Tully, RHIT
Margie White, MS, RHIA, NHA, CPHQ
Melinda Wilkins, MEd, RHIA
Pat Wilson, ARRT, CPC, PMP
Theresa Wisdom, MBA, RHIA

AHIMA staff

Harry Rhodes, MBA, RHIA, CHPS, CPHIMS, FAHIMA
Beth Hjort, RHIA, CHPS
Maggie Williams, AM
Rita Scichilone, MHSA, RHIA, CCS, CCS-P, CHC

Special thanks to

Lori Youngberg, RHIA

This work was supported in part by a grant to the Foundation of Research and Education from 3M Health Information Systems and Just Associates.