State Level Health Information Exchange

Final Report Part II: Coordinating Policies That Impact Access, Use, and Control of Health Information

Contract Number: HHSP23320074100EC

March 10, 2008

Prepared for:
Department of Health and Human Services,
Office of the National Coordinator for Health Information Technology (ONC)

© FORE 2008

Foundation of Research and Education of American Health Information Management Association
233 N. Michigan Ave., 21st Floor
Chicago, IL 60601-5800
phone: (312) 233-1100
fax: (312) 233-1090
www.ahima.org/fore
Findings and Recommendations from the State Level Health Information Exchange Consensus Project March 2008

State Level Health Information Exchange: Coordinating Policies that Impact the Access, Use, and Control of Health Information

Final Report Part II

Contract Number: HHSP23320074100EC
March 10, 2008

Foundation of Research and Education of the American Health Information Management Association
233 North Michigan Avenue, 21st Floor
Chicago, IL 60601

© FORE 2008
# Table of Contents

Acknowledgments ..........................................................................................................................3  
Executive Summary .......................................................................................................................5  
  Introduction ..............................................................................................................................5  
  Background and Methodology .................................................................................................6  
  Key Findings and Observations ...............................................................................................7  
Introduction ....................................................................................................................................9  
  Project Goals and Objectives .................................................................................................10  
  Project Scope and Requirements .............................................................................................11  
  Data Access, Use, and Control Issues: Previous Analyses and Projects ...............................12  
  Mining for Obstacles to Successful HIE ..................................................................................14  
Methodology .................................................................................................................................16  
  Description of the Methodology ............................................................................................16  
  Scenario Used in This Project .................................................................................................18  
    Main Scenario ..................................................................................................................18  
    Alternative 1 .....................................................................................................................19  
    Alternative 2 .....................................................................................................................19  
    Alternative 3 .....................................................................................................................19  
  Flexibility of the Scenario ......................................................................................................19  
  Key Features of the Scenario Used in This Project ...............................................................20  
    Pertinent Use Cases ..........................................................................................................20  
    Constraints Placed on the Optionality in the States and HIEs Involved ..........................20  
Results ...........................................................................................................................................23  
  Findings, Implications, and Recommendations .....................................................................23  
Conclusions ...................................................................................................................................28  
  Conclusions and General Principles ......................................................................................28  
  Methodology Proven Useful ...................................................................................................28  
  Results Were Found in the Expected Areas ...........................................................................28  
  Tighter Front-End Controls May Save Effort on Back-End Processes ..................................28  
  Findings, Implications, and Recommendations Generate a Valuable Discussion ..................29  
  Recommendations for Future Action ....................................................................................29  
References .....................................................................................................................................30  
Appendix: Preliminary Questions to Analyze Influences on Access, Use, and Control............32
Acknowledgments

Steering Committee
Laura L. Adams, CEO, President and CEO, Rhode Island Quality Institute, Providence, RI
Antoine Agassi, Director and Chair, State of Tennessee eHealth Council, Nashville, TN
Rachel Block, Executive Director, New York e-Health Collaborative, New York, NY
Ray Campbell, Esq., MPA, CEO, Massachusetts Health Data Consortium, Waltham, MA, Chair
Devore S. Culver, Executive Director, HealthInfoNet, Manchester, ME
Lynn S. Dierker, RN, Senior Advisor and Member, Board of Directors, Colorado Regional Health Information Organization, Denver, CO
Donald L. Holmquest, MD, PhD, JD, CEO, CalRHIO, San Francisco, CA
Marc Overhage, MD, PhD, FACP, FACMI, Director, Medical Informatics, Regenstrief Institute, Inc.; CEO, Indiana Health Information Exchange, Inc.; and Associate Professor of Medicine, Indiana University School of Medicine, Indianapolis, IN
Jan Root, PhD, Executive Director, Utah Health Information Network, Murray, UT
Christopher Sullivan, Administrator, Office of Health Information Technology, Agency for Health Care Administration, Tallahassee, Florida Health Information Network
Roxane Townsend, MD, Assistant Vice President of Health Systems, Louisiana State University, Baton Rouge, LA

Research Project Team
AHIMA (Part II HIE Policies and Practices)
Don Mon, Vice President, Practice Leadership, AHIMA
Harry Rhodes, Director, Practice Leadership, AHIMA
Lydia Washington, Director, Practice Leadership, AHIMA

Manatt Health Solutions (Part I Governance and Sustainability)
William Bernstein, Partner, Manatt Health Solutions
Lammot du Pont, Senior Manager
Kalpana Bhandarkar, Senior Analyst
Allison Garcimonde, Senior Analyst
Kerry Griffin, Senior Policy Analyst
Julie Murchinson, Managing Director

Project Staff
Project Director
Lynn S. Dierker, RN

Foundation of Research and Education (FORE) Staff
Linda L. Kloss, MA, RHIA, CEO, American Health Information Management Association
Eileen M. Murray, MM, CFRE, CAE, Vice President and Executive Director, Foundation of Research and Education
Office of the National Coordinator for Health Information Technology (ONC) Staff

Kelly Cronin, Director of the Office of Programs and Coordination
Christopher Muir, Senior Program Analyst
Betsy Ranslow, Senior Policy Analyst

Project Partners

eHealth Initiative (eHI)
Janet M. Marchibroda, CEO, eHealth Initiative and Executive Director, eHealth Foundation
Christine Bechtel, Vice President, Public Policy and Government Relations

Healthcare Information and Management Systems Society (HIMSS)
H. Stephen Lieber, CAE, President and CEO
Pamela V. Matthews, RN, BSIE, MBA, FHIMSS, Director, Information Management Systems
Patricia Wise, RN, MSN, MA, FHIMSS, Vice President, Healthcare Information Systems

National Conference of State Legislatures (NCSL)
Donna Folkemer, Group Director, Forum for State Health Policy Leadership
Executive Summary

Introduction

The State-Level Health Information Exchange (HIE) Consensus Project (Project) began in 2006 under a contract from the Office of the National Coordinator for Health Information Technology (ONC) with the Foundation of Research and Education (FORE) of the American Health Information Management Association (AHIMA). The Project is focused on bringing forward relevant field research, guiding ongoing HIE development among states, informing federal-level HIE strategies, and helping to align multilevel efforts to establish a nationwide health information network (NHIN). It is accomplishing this goal through dissemination of field research and guidance materials and broad stakeholder dialogue. A Steering Committee composed of leaders from a mix of state-level HIE entities plays a pivotal role to guide and contribute to research and analysis and to formulate Project recommendations for advancing HIE development.

Project activities carried out between March 2006 and January 2007 produced a series of reports and guidance for emerging state-level HIE initiatives and federal HIE strategies.

- **Development of State Level Health Information Exchange Initiatives Final Report, September 1, 2006.** Outlines the distinct value and characteristics of state-level HIE development and includes an initial set of recommendations for state, federal and private-sector activities to advance state-level HIE initiatives.
- **Development of State Level Health Information Exchange Initiatives Final Report: Extension Tasks, January 2007.** Presents research findings and recommendations related to four areas: the relationship between state-level HIEs and federal activities, analysis of HIE projects that have achieved financial sustainability, roles and influence of public payers on state-level HIE activities, and roles of state-level HIEs in quality improvement and reporting.
- **State Level Health Information Exchange Initiative Development Workbook: A Guide to Key Issues, Options and Strategies, February 2007.** Established a resource for state-level HIEs including practical policy and practice guidance for establishing state-level HIE governance, structure, operations, finance, and HIE policies. Provides profiles of the state-level initiatives represented on the Project’s Steering Committee.

All of the Project’s reports and the Workbook are publicly available at [www.staterhio.org](http://www.staterhio.org).

The Project embarked on its second phase of work in March 2007 to continue examination and analysis of evolving state-level HIE issues. Activities included continued field research and analysis into dimensions of state-level HIE, facilitating stakeholder input, and developing options for structuring state-level HIE as part of a nationwide network, including defined HIE-related roles and accountabilities.

Research was organized into three tasks.

1. To further examine the evolving functions and governance structures of state-level HIE initiatives
To identify sustainability considerations related to these HIE roles, services, and business models
3. To identify the challenges in crafting consistent data access, use, and control policies and practices across HIEs

The Final Report from the 2007 Project is divided into two separate documents. Part I of the Final Report addresses Tasks 1 and 2 and includes findings related to state-level HIE governance and sustainability considerations, as well as recommendations related to state- and federal-level HIE strategies.

This Part II of the Final Report represents a synthesis of current research findings, analysis, and recommendations related to the Project’s Task 3 research. It examines the challenges faced by HIE organizations in coordinating implementation of consistent policies and practices pertaining to the access, use, and control of health information.

**Background and Methodology**

A number of local, state-level and HIE entities participating as contractors in the NHIN are entering the trial implementation stage. Anticipating their challenges and identifying practical solutions will increase operational efficiency and contribute to a likelihood of success in establishing sustainable data exchange. Some of the most difficult challenges facing HIEs relate to structuring data access, use, and control policies and procedures, particularly in the following six areas: access management, authentication, subject and user identity arbitration, management of consumer choices to not participate in the network, availability of access and disclosure information regarding a consumer's personal health record (PHR) and HIE data, and routing of consumer requests to correct data.

These aspects of data exchange generate numerous and complex issues that are compounded by the number of factors that affect them. These include health policy; federal and state laws, rules, and regulations; technical standards; HIE architecture and operational policies and procedures; business practices and agreements; business models; and presence of a governance structure, such as that provided by a state-level HIE organization, that effectively coordinates and oversees these factors.

Previous analyses and existing projects, such as the Connecting for Health Common Framework, NHIN prototypes, the Health Information Security and Privacy Collaborative (HISPC), and the Health Information Technology Standards Panel (HITSP), have already identified a number of access, use, and control issues that may hinder the exchange of health information. The intent of this research and analysis is to add value to previous work and identify the obstacles to successful data exchange or threats to the business models of HIE entities caused by the interaction among the six aforementioned areas of access, use, and control and the multiple factors that affect them.

A multidimensional analysis of these factors at the operational level can produce specific and detailed findings, and, more importantly, indicate how operational policies and procedures, data use and reciprocal support agreements, service level agreements, privacy laws, and technical standards may need to be constructed or modified. The practical solutions that these implications might suggest can then be implemented proactively by HIEs, and, thus, help to avoid some of the pitfalls identified in this report. This premise is the basis for, and value of, this project.

The specific goals and objectives of this project are to:
• Examine the current landscape of HIE access, use, and control policies and practices at the national, state, and local levels
• Identify access, use, and control issues specifically related to state-level HIE roles, functions, policies, and practices
• Identify specific points in the HIE process flow where any of the six target areas of access, use, and control are affected by the interaction of multiple factors and describe how HIE may be hindered by one or more of these effects
• Identify the implications for access, use, and control policies and practices, as well as for health policy; federal and state laws, rules, and regulations; technical standards; HIE architecture, policies, and procedures; business agreements, practices, and models; and state-level HIE roles when access, use, and control are affected by these factors
• Identify the potential threats to HIE business models when access, use, and control are affected by these factors
• Develop appropriate high-level and detailed recommendations
• Develop a set of preliminary questions and a methodology that can be used in future studies as a framework for analyzing the complexity of the issues

Given the number and complexity of the issues surrounding the six target areas of access, use, and control, a methodology was developed to analyze a realistic HIE scenario, mining it to address the above goals and objectives. Key components of the methodology include: (1) development of a composite scenario that embodies the data management issues identified as priorities for this analysis; (2) a preliminary set of mining questions that could be used to explore the interaction of various factors and their effects on the six targeted areas of access, use, and control; and (3) a structured walk-through of the scenario to conduct a multidimensional analysis. The scenario that was composed involved the need to access registration summary information and medication history data, as well as laboratory results—use cases deemed to be immediately relevant to state-level HIE and NHIN trial implementers.

**Key Findings and Observations**

Application of this methodology produced a number of complex findings, implications, and recommendations. These were organized according to the four major stages of the scenario: (1) preliminary steps related to requesting information (registration summary and medication history data, as well as laboratory results); (2) requesting and receiving registration summary and medication history data; (3) requesting and receiving laboratory results; and (4) follow-up steps after requesting and receiving the information including patients verifying that the information imported into their PHRs is correct and patients requesting corrections to data.

Example 1 revealed how master patient index (MPI) contamination can spuriously populate HIE systems with inaccurate data and how responding HIEs can send inadvertently erroneous data to requesting HIEs as a result. A number of implications arose, including whether there should be a mechanism for the requesting HIE to notify the responding HIE that it received erroneous data and whether there is any responsibility on the part of responding HIE to take action to improve the data quality of the MPI after receiving such notification. Lastly, it was pointed out that improving the MPI's data quality on the front end could avoid consumer requests to correct data on the back end, saving HIEs time and resources to make such corrections.
Example 2 dealt with the issue of a consumer choosing not to participate in the network. This example pointed out how confusion will occur because such a choice may return no health information to the requesting HIE. The critical aspect is whether an explanation should accompany the message explaining why there is no health information to return. Without an accompanying explanation, the requesting HIE may not know whether there is no actual health information to return; there is no health information to return because the consumer has elected not to participate in the network, but health information truly exists and can be accessed directly from the source care delivery organization (CDO); or there is a state law preventing the responding HIE from sending the requested health information. Interestingly, Example 2 highlighted how differences in HIE architecture would cause state-level HIEs and local HIEs to address the issues differently.

Example 3 described how consent directives implemented across multiple CDOs, local HIEs, and state-level HIEs can potentially cause conflicts among patient consents. The example discussed ways in which such conflicts can be reconciled. Lastly, the example pointed out how minimizing conflicts in consent directives on the front end can avoid the time and resources to correct them on the back end, thereby enhancing provider and consumer perceptions of the quality of HIE operations.

A number of conclusions and general principles can be gleaned from the results of these three examples, including the following: (1) the methodology was proven to be useful and could be implemented in the field, as well as serving as a framework for future studies of this nature; (2) tighter front-end controls may save effort on back-end processes; and (3) the analysis of the findings, implications, and recommendations generates a discussion that is equally as valuable as the results themselves and can spur multiple stakeholders in the field to find practical solutions appropriate for them.

Given the usefulness of the methodology and value of the findings, the following actions are recommended:

- The findings, implications, and recommendations and the methodology should be distributed to the NHIN contractors so that they can factor them into their trial implementations.
- There is much synergy between the state-level HIE and the NHIN trial implementers. There is an opportunity to take advantage of the leverage that can be obtained through collaborative efforts. The state-level HIEs and the NHIN trial implementers should plan on ways to collaborate with each other.
- Given the time and resource constraints of this project, many of the ways in which the factors interacted with the six areas of access, use, and control were not analyzed. Further funding should be provided to continue this effort.
Introduction

Data access, use, and control issues are some of the most difficult to address both in the actual exchange of health information and in protecting the privacy of the individual and the confidentiality of health information. Handling the sheer number of issues (see Table 1) and analyzing the complexities of each issue (see the list of Preliminary Questions in the Appendix) is indeed a challenging task.

Table 1
A Sampling of Issues Related to Data Access, Use, and Control

Access: Who Has Authorized Access to What Data
- Who determines what data can be accessed and by whom?
- What are the rights of access for the individual to whom the data pertains?
- What are the rights and responsibilities of providers and caregivers who access health data?
- What are the rights and responsibilities related to access by nonprovider users or those using data for nondirect care purposes (e.g., quality reporting, administrative, research, public health, population health, biosurveillance)?

Use: For What Purposes Can Authorized Individuals Use the Data?
- Who may mine or manipulate data?1
- Who may sell data?1
- Who may disclose or publish data?1
- Who must pay to access, use, publish, or sell data?1
- Who is required to disclose data in response to subpoenas or court orders?1
- Are data sufficiently anonymized or deidentified when used for nondirect care purposes?

Control: How Are Data Validity and Accuracy Ensured?
- How is accuracy of patient identity ensured?
- How are records accurately linked across networks?
- Who can amend health data?
- How are disclosures authorized and tracked?
- What audit controls are in place for data security, integrity, and accuracy?


Other items above were derived from the AHIMA Electronic Health Information Management (e-HIM) Workgroup on HIM in HIE. HIM Principles in Health Information Exchange. *Journal of AHIMA* 78, no.8 (September 2007): 69-74.
The complexity in data access, use, and control issues is further compounded by a number of factors that affect them, including health policy; federal and state laws, rules, and regulations; technical standards; HIE architecture and operational policies and procedures; business practices and agreements; business models; and the roles of state-level HIEs (See Figure 1).

### Project Goals and Objectives

Previous analyses and existing projects, such as the Connecting for Health Common Framework, NHIN prototypes, HISPC, and HITSP, have already identified a number of data access, use, and control issues that may hinder the exchange of health information. The intent of this project is to go a level deeper and identify the obstacles to successful data exchange or threats to the business models of HIEs caused by the interaction among six specific areas of access, use, and control and the multiple factors that affect them (identified in Figure 1).

Except for the few HIEs that are already in operation, most HIEs are in the organizational development phase or are moving from the prototype to the trial implementation phase. Although many HIEs naturally are focusing on exchanging data within the HIE, few, if any, are exchanging data between HIEs. Yet, to build the NHIN, exchanging data between HIEs is exactly what must occur. To help ensure the success of data exchange between HIEs, it is important to anticipate how such issues as data access, use, and control will be affected by a variety of factors. A multidimensional analysis\(^1\) of these factors at the operational level can produce specific and detailed findings and, more importantly, indicate how operational policies and procedures, data use and reciprocal support agreements (DURSAs), service level agreements (SLAs), privacy laws, and technical standards may need to be constructed or modified. The practical solutions that might be suggested by these implications can then be implemented proactively by HIEs and, thus, help them

---

\(^1\) The term *multidimensional analysis* here implies that multiple factors were considered simultaneously from a qualitative standpoint. It is not used in the quantitative or classical statistical analysis sense.
to avoid some of the pitfalls identified in this report. This premise is the basis for, and value of, this project.

The specific goals and objectives of this project are to:

- Examine the current landscape of HIE data access, use, and control policies and practices at the national, state, and local levels
- Identify data access, use, and control issues specifically related to state-level HIE roles, functions, policies, and practices
- Identify specific points in the HIE process flow where any of the six target areas of data access, use, and control are affected by the interaction of multiple factors (identified in Figure 1) and describe how HIE may be hindered by one or more of these effects
- Identify the implications for data access, use, and control policies and practices, as well as for health policy; federal and state laws, rules, and regulations; technical standards; HIE architecture, policies, and procedures; business agreements, practices, and models; and state-level HIE roles—that is, how they may need to be constructed or modified—when access, use, and control are affected by these factors
- Identify the potential threats to HIE business models when access, use, and control are affected by these factors
- Develop appropriate high-level and detailed recommendations
- Develop a set of preliminary questions and a methodology that can be used in future studies as a framework for analyzing the complexity of the issues

**Project Scope and Requirements**

The project’s scope and requirements are as follows:

- A scenario should be developed that highlights two use cases currently under NHIN trial implementation—registration summary and medication history (ONC, 2006b) and laboratory results reporting (ONC, 2006c)—to achieve the above goals and objectives.
- The scenario must be realistic, not contrived simply to fit access, use, and control issues and other factors that must be addressed.
- The scenario must also be immediately relevant to all HIEs, but particularly to state-level HIEs and NHIN trial implementers, so that they may be able to avoid in their current projects some of the pitfalls identified in this project. A scenario is relevant when it reflects an immediate concern for state-level HIEs and NHIN trial implementers and supports their business case.
- The scenario must illustrate a HIE-to-HIE data transfer, where the HIEs involved could be any combination of the following:
  - A HIE that complies with a NHIN prototype architecture
  - A HIE that is cooperating with or is itself a state-level HIE
  - A private nongeographically bound HIE (e.g., the Veterans Health Administration)
  - A health record data bank or other network-based data source (e.g., a Web-based PHR system).
- The scenario should feature a PHR that is connected to a HIE as another source of health information.
The access, use, and control issues to be explored must be limited to the following six areas and their key components, which are of immediate interest to state-level HIEs and the NHIN trial implementers:

- Access management: identity proofing, assigning access privileges, terminating access, and providing emergency access
- Authentication: where requirements may differ, or where one HIE may need to rely on differing levels of authentication (or authentication strength)
- Subject and user identity arbitration: how varying approaches can be reconciled (e.g., what do HIEs do if they are not able to arbitrate an identity)
- Management of consumer choices to not participate in the network
- Availability of access and disclosure information regarding a consumer's PHR and HIE data
- Routing of consumer requests to correct data.

Not all six target areas of access, use, and control may be pertinent in any given scenario. Given project time and resource limitations, not every law, standard, architecture type, HIE policy and procedure, business or service level agreement, role, or other factor can be explored. A completely exhaustive set of findings and implications is not expected to be produced.

Because not every target access, use, and control issue, nor every implication, will be explored, a set of preliminary questions coupled with a methodology should enable HIEs to explore such issues and implications in the field, as well as enable future studies of this type to be conducted.

Access, use, and control issues that are not part of the six target areas above, but are uncovered serendipitously, should still be reported.

Data Access, Use, and Control Issues: Previous Analyses and Projects

Until recently, data access, use, and control issues have been characterized as data ownership, an umbrella concept embodied in the question, “who can do what to which data under what circumstances?” (Waller & Alcantara, 1998) However, the question of who owns the data has become less useful because no single person, whether the healthcare provider or the patient, has ever had “exclusive ownership over health information, where ownership is defined as the ability to exercise complete sovereignty over information—to disclose, sell, destroy, alter, or determine who shall have access to it.” (Burrington-Brown, et al, 2007; Waller & Alcantara, 1998)

Breaking down the concept of data ownership into its component parts—access, use, and control—is more useful because it is easier to separate their influences and develop practical solutions to the issues. Previous reports and existing projects have done an excellent job in addressing a number of data access, use, and control issues when taking this approach.

The Gartner report (2007) on NHIN prototype architectures broke down the access, use, and control process into the following components:

- Arbitrate identity
- Identify subject
- Locate records
- Maintain consumer data-sharing permissions
- Maintain registries of NHIN-participating systems and organizations
• Manage data selection parameters for secondary data use
• Provide consumer access to access and disclosure logs
• Provide data to secondary users
• Pseudonymize and reidentify patient data
• Publish PHR location
• Retrieve data
• Route consumer requests to correct data
• Route data
• Route data on the basis of consumer-specified preferences

They then described how each of the four NHIN prototypes addressed access, use, and control issues within their network through these components. Accenture, for example, provided facilities for cross-indexing patients and providers and for locating patient records in their prototype. The MPI coupled with authorization and authentication addressed access management and user and subject identity matching issues for the HIE.

As for harmonizing interoperability standards that support access, use, and control processes, HITSP published a series of technical notes and transaction packages, the latter of which describe the context and constraints in which standards are used. Among the series is an access control transaction package (HITSP, 2007a), a manage consent directives transaction package (HITSP, 2007d), and a security and privacy technical note (HITSP, 2007f).

From a technical standpoint, HITSP consent directives provide an interesting approach to managing consents. A consent directive is essentially a record of a consumer’s privacy policy that specifies to one or more healthcare entities which operation to perform (e.g., access, use, disclose, amend), within a specified period of time, for a specific purpose (treatment, payment, operation, other data use), under certain conditions and contexts (e.g., unconscious in an emergency room). One or more consent directives can be created, updated, and stored in a repository, and any consent directive within the repository that applies to the situation in which a consumer is being treated can be used proactively because the consumer has already specified the conditions in which the consents can be used. Although elegant in concept, consent directives are not yet widely implemented, and it will be interesting to observe how well they facilitate workflow as a result of consents having already been obtained and how well consents are managed over time and multiple provider settings.

Through their variations, implementation, and nationwide summary reports, the HISPC project produced a wealth of material on access, use, and control through the lens of state privacy and security laws, rules, regulations, and business practices (Dimitropoulos, 2007a-d). In addition to surfacing the issues, the HISPC project provided a number of recommendations on how to address access, use, and control issues, albeit primarily at the health policy or state level. Moreover, a handful of HISPC states appear to be considering adopting the methods to manage consent directives put forth by HITSP.

The Certification Commission for Healthcare Information Technology (CCHIT) has drafted a number of criteria to certify HIE networks for core and modular capabilities starting in October 2008 (CCHIT, 2008). While still in draft form, the current plan is that HIEs seeking certification will be required to comply with all security criteria (core capability), and either the Health Level 7 (HL7) Continuity of Care Document (HL7, 2007) or the laboratory transaction set (modular capabilities).
Finally, the Connecting for Health Common Framework (2008) reviewed a number of factors that affect access, use, and control. The framework provides policy and technical guides on such areas as the architecture for privacy in HIE, patient matching, authentication, and audit trails, among others. Among their policy guides is a model set of HIE policies and procedures and, as it relates to this project, technical guides on medication history and laboratory results standards.

An interesting aspect of the Connecting for Health Common Framework is the concept of a record locator service (RLS), which leaves data where they are in CDO systems (Connecting for Health, 2006b, Gartner, 2007). The RLS provides authorized users with the location of the clinical data sources so that a HIE can know which data sources to access for the health information needed by the requesting HIE. This architecture ostensibly enables users to access health information without the need for a national patient identifier or a centralized database at the HIE level (though not precluding them) and would presumably enforce greater privacy protections (Connecting for Health, 2006a).

The above projects addressed access, use, and control issues in HIE thoroughly and clearly. They were stellar in the manner in which they raised issues and, in some cases, designed and tested solutions. The findings from these projects provided an excellent foundation, as well as a point of departure, for this project.

**Mining for Obstacles to Successful HIE**

As previously mentioned, it is important to anticipate barriers to the HIE process which may be caused by lack of agreements for how data access, use, and control will be managed by data-sharing participants. HIE entities must find practical solutions to these kinds of challenges. To provide guidance that could be relevant to the realistic dimensions of data sharing across HIE environments, a fine-grained analysis was required for this project. It was important to analyze the effects of multiple factors (the interaction of multiple rows, multiple columns, or rows and columns in Figure 1) rather than the effects of a single dimension (an individual row or column in Figure 1).

For example, a higher level finding—such as a consumer opting out of network participation would cause the responding HIE to reply to the requesting HIE with a message stating “no health information to return”—although useful, is not detailed enough to satisfy the requirements of this project. To provide practical solutions, this project had to ask more granular questions, such as:

- If there is no health information to send to the requesting HIE because the consumer has elected not to participate, how will the requesting HIE know there was no returned health information because there is:
  - No actual health information to transfer
  - No health information to transfer because the consumer has elected not to participate, but valid health information truly exists at one or more CDOs participating in the HIE
  - Some other error in the network that might be an artifact of the HIE architecture (e.g., the responding HIE deploys a central repository and the repository incorrectly associated no pertinent health information to the consumer)
  - An error at the CDO level (e.g., the CDO’s MPI incorrectly associated the wrong or no health information to the consumer) causing the HIE to reply with no health information to return
• A state law that prohibits sending the type of health information that is specifically requested
• Should a notice, perhaps coming directly from the consumer’s consent directive, be sent to the requesting HIE stating the reason for the no return so that the provider is not left to question the value of HIE (threat to the business model), or more importantly, be influenced in a way that might affect the care of the patient?
• Will such a notice inadvertently communicate something about the patient and violate a privacy and confidentiality principle?
• Is there a privacy or confidentiality reason why a consumer might elect to not participate in the network as a means for exchanging health information but agree that the providers can directly communicate with each other? Will that decision affect the business model of a HIE?
• Is there a HIE operational policy or procedure that could inadvertently prevent a responding HIE from providing information to the requesting HIE?
• What is required of the CDO to ensure that health information is of a certain level of data quality before it is passed on to its HIE and thus not put the HIE in a position of sending erroneous replies to the requesting HIE?
• What is required of the HIE to ensure that its records, no matter its network architecture (e.g., central repository or RLS), are at a certain level of data quality such that it will send accurate replies to requesting HIEs?
• What should be contained in a DURSA among HIEs, the policies and procedures of a HIE, and/or the SLAs between a HIE and participating CDOs to address these issues?
• What is the role of a convening state-level HIE in ensuring that its contracted local HIEs agree to the relevant components of DURSAs, operational policies and procedures, or SLAs?
• What is the responsibility of a coordinating or implementer state-level HIE in developing, managing, or executing the relevant components of DURSAs, operational policies and procedures, or SLAs?
• What is the role of the HIE to systematically inform HITSP or the states that a standard or state privacy law needs to be (better) harmonized to eliminate an access, use, or control barrier?
• Is there a technical standard that conflicts with health policy or privacy law, or absent public policy, has the potential to introduce a patient safety error inadvertently?
• Should a standards development organization (SDO) have a mechanism to limit its standards consistently so that those standards do not go beyond or get ahead of health policy?
• What is the role of a SDO to elevate such issues to policy makers when it discovers them and to collaborate on the resolution of the issues (with the assumption that such resolution will then make its standards more consistent with policy)?

These questions illustrate that, when other factors are considered, a single access, use, or control issue raises a whole host of implications at the operational level. To add to the complexity, these implications can surface from more than one direction. For example, these questions surfaced in considering the implications of a consumer opting not to participate in the network. However, some of these questions could have been surfaced easily by looking at the particular architecture of a HIE, state privacy laws, a technical standard, and other factors in Figure 1.
Methodology

Description of the Methodology

As described above, a mining approach was needed to (1) determine where in the process HIE could be hindered by factors affecting access, use, and control and (2) identify their implications. To that end, the following methodology was developed:

- **Conduct an environmental scan on access, use, and control issues from previous projects to avoid duplication in this project. Gain a better understanding of how multiple factors interact with each other to affect access, use, and control.**

Previous analyses or projects (e.g., Connecting for Health, NHIN prototypes, HITSP, HISPC, CCHIT) identified factors that affected access, use, and control. To ensure that this project would not duplicate the findings of those projects, and to gain an in-depth understanding of how the interaction of these factors could affect access, use, and control, the project team reviewed relevant materials on these factors. In addition, subject matter experts (SMEs) were consulted or were resident on the project team. The factors and the materials reviewed are listed in Table 2. Given the project’s time and resource limitations, the materials reviewed are certainly not exhaustive. However, they do represent the breadth and depth of access, use, and control issues well, and they provided sufficient information to conduct in-depth analyses on the interactions among the factors.

<table>
<thead>
<tr>
<th>Factor</th>
<th>Materials Reviewed/SME Consulted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Federal laws, rules, and regulations</td>
<td>• HIPAA</td>
</tr>
<tr>
<td></td>
<td>• Confidentiality of Alcohol and Drug Abuse Patient Records, 42 CFR Part 2</td>
</tr>
<tr>
<td>State laws, rules, and regulations</td>
<td>• HISPC final variations, implementation, and summary reports (Dimitropoulos, 2007a-c)</td>
</tr>
<tr>
<td></td>
<td>• HISPC reports reflecting state-level issues (Dimitropoulos, 2007d)</td>
</tr>
<tr>
<td>Technical standards, certification</td>
<td>• Pertinent HITSP interoperability specifications, technical notes, and transaction packages (HITSP, 2007a-g)</td>
</tr>
<tr>
<td>criteria</td>
<td>• Pertinent HL7 standards (HL7, 2007)</td>
</tr>
<tr>
<td></td>
<td>• CCHIT draft network certification criteria (CCHIT, 2008)</td>
</tr>
<tr>
<td>HIE architecture</td>
<td>Gartner report (2007) on NHIN prototype architectures</td>
</tr>
<tr>
<td>HIE policies and procedures</td>
<td>DURSA, December 20, 2007, Draft 4 (ONC, 2007)</td>
</tr>
<tr>
<td>HIE business practices and models</td>
<td>Previous state-level HIE reports published by FORE (FORE 2006a-b, 2007a-b)</td>
</tr>
<tr>
<td>State-level HIE roles</td>
<td>Previous state-level HIE reports published by FORE (FORE 2006a-b, 2007a-b)</td>
</tr>
</tbody>
</table>

- **Develop a composite scenario from those used in previous projects**

A high-level, composite scenario (see the Results section) was derived from the AHIC emergency responder (ONC, 2006a), registration and medication history (ONC, 2006b), and laboratory results reporting (ONC, 2006c) use cases, their counterpart HITSP use cases
(HITSP, 2007b, 2007e), the 2008 public comment version of CCHIT’s draft network certification criteria (CCHIT, 2008), and the Gartner report (2007) on NHIN prototype architectures. Selecting these use cases helps align this project with existing major federal initiatives. Further, the registration and medication history and laboratory results reporting use cases were thought to be immediately relevant to both state-level HIEs and NHIN trial implementers.

The composite scenario was further informed by HIE use case scenarios developed from the health information management perspective (AHIMA, September 2007c).

- **Develop a preliminary set of mining questions that could be used to explore the interaction between the factors and their effects on the six target access, use, and control areas.**

A set of mining questions (for examples, see “Mining for Obstacles to Successful HIE” in the Introduction section) were derived after reviewing the materials listed above, as well as from documents on health information management principles in HIE (AHIMA, 2007; AHIMA, September 2007a-c; Just & Durkin, September 2007; Just, 2008). These questions were then grouped according to the six target access, use, and control areas (see Figure 1), which essentially formed a rough structure of the analysis to be performed in the walk-through of the scenario in the next step. The entire set of preliminary mining questions can be found in the Appendix.

- **Conduct the multidimensional analysis via a structured walk-through of the scenario. Raise one or more of the preliminary questions as a means of identifying detail findings and their implications for laws, standards, or HIE business models and operations, including practices, policies, procedures, and various forms of agreements.**

This step involved a structured walk-through of the scenario, examining the interaction between the factors and their effects on access, use, and control at each point in the flow of information between HIEs. At each point, one or more of the preliminary mining questions is raised. As was found during the actual process, the preliminary mining questions either immediately uncovered an obstacle to access, use, or control caused by one or more of the factors or generated another set of more specific questions that resulted in a deeper analysis of the issues at that point.

For example, the scenario in this project was deliberately constructed so that the responding HIE deploys a MPI. In the structured walk-through, when the point is reached at which the HIE must access its MPI for matching a patient to his or her records (a HIE architecture factor), one preliminary question that can be raised is, “what is the contamination rate of the MPI?” Applied to the specific point in the walk-through, that preliminary question generates a number of other, more specific questions, such as:

- How does MPI contamination rate (duplicate records, missing data, erroneous data, etc.) affect subject identity arbitration in this scenario? Would MPI contamination not be a factor if a different HIE architecture were involved?
- Could a contaminated MPI cause data to be associated erroneously with an individual? Would the HIE then be sending erroneous data to the requesting HIE?
• Did the contamination occur at the HIE level, or was erroneous information passed to it from the CDO, causing the HIE’s MPI to be contaminated and result in cascading errors?
• What terms in the business agreement or contract between the HIE and participating CDOs must be in place to address this situation?
• What terms in the DURSA among HIEs must be in place to address this situation?

The answers to these questions produce:

• A specific finding: Contaminated MPIs can cause the HIE to send erroneous data
• One or more implications: The HIE will need to have some form of agreement with its participating CDOs and the HIEs it exchanges data with to address data quality and other business concerns
• One or more specific recommendations: The HIE should consider putting in its SLA with participating CDOs a mechanism to monitor data quality, as well as a term in the agreement about the practices and time frame to rectify the errors

• Document and report the findings, implications, and recommendations.

The findings, implications, and recommendations were then cross-checked with those from previous analyses and projects to ensure there were no duplications and to confirm the accuracy of facts (e.g., a criterion, a standard specification) extracted from them. To the extent possible, the findings, implications, and recommendations were also cross-checked with personnel from those projects. When these cross-checks were completed, the findings, implications, and recommendations were then documented and reported.

Scenario Used in This Project

The results for this project were based on the following scenario. Note that the scenario is written to enable maximum optionality because it must be flexible enough to facilitate variation among the multiple factors. In this section, the scenario is presented along with a description of its flexibility. The findings, implications, and recommendations immediately follow. Although the scenario contains aspects of the AHIC emergency responder, registration and medication history, and laboratory results use cases, for scoping purposes the project focused only on the latter two.

Optionality in the scenario, distinguished by italics, enables what-if comparisons when conducting the analysis. For example, one could ask, “what if the states involved were Wisconsin and California, instead of New York and California? How would variation in state laws differentially affect access, use, and control?” The benefits of optionality will be described after this scenario.

Main Scenario

Jane Doe and her boyfriend of six months, John Q. Public, both residents of state 1, travel to state 2 for a vacation. While on vacation, they are involved in an automobile accident. The first responder is a law enforcement officer. The officer finds Ms. Doe severely injured and unconscious. Mr. Public is conscious and appears to be only slightly injured with cuts and bruises. The officer immediately calls the emergency dispatch center, administers first aid, and attempts to access Ms.
Doe’s PHR. The emergency medical technicians (EMTs) arrive, begin triage, and then transport the couple to the nearest hospital.

Alternative 1

While in transit, the EMTs attempt to access both individuals’ PHRs. Mr. Public is able to provide access to his PHR to the EMTs. However, when asked about Ms. Doe’s, he states he does not know whether she has one since they never discussed the topic in the time they have known each other.

Alternative 2

At the hospital, emergency department (ED) personnel attempt to access both individuals’ PHRs. Mr. Public is able to provide access to his PHR to the ED personnel. However, when asked about Ms. Doe’s, he states he does not know whether she has one since they never discussed the topic in the time they have known each other.

Alternative 3

At the hospital, the emergency physician questions Mr. Public regarding the medical history of Ms. Doe. Mr. Public recalls that Ms. Doe takes medications to manage a number of chronic conditions, but he does not know exactly what those medications are. Suspecting a condition or trauma, the emergency physician requests a medication history and the most recent laboratory results for Ms. Doe through the CDO’s electronic health record (EHR) or through the HIE and/or state-level HIE in which the CDO participates from the HIE and/or state-level HIE of state 1, where Ms. Doe resides and has received previous care. Upon accessing her records, the sending HIE notes that Ms. Doe has elected to mask information in her medical record, a right given to her from her state’s patient permissions law.

Flexibility of the Scenario

Given the multidimensional requirements for this analysis, the scenario was deliberately constructed so that variability in each of the factors has an opportunity to manifest itself. For example in this scenario, any state can be inserted in as state 1 or state 2. After the states have been selected, the characteristics of those states are then inherited in the scenario.

Thus, if Jane Doe and John Q. Public were residents of New York (state 1) and traveled to California (state 2), then the scenario has to deal with New York’s and California’s state-level HIE governance and operations model (New York eHealth Collaborative [NYeC] and California Regional Health Information Organization [CalRHIO], respectively), its HIE architecture, and state laws. Further, depending on the hospital to which Jane Doe and John Q. Public were taken, the scenario has to consider attributes of the local HIE in which that hospital participates—its architecture, policies and procedures, and agreements—and their relationship to the state-level HIE, if the local HIE participates in the state-level HIE. In the example here, if Ms. Doe or Mr. Public were taken to the hospital in either Santa Cruz or Mendocino County, CA, the scenario would have to account for the specific architecture of the local HIE (Northrup Grumman or Computer Science Corporation [CSC] prototype, respectively) and CalRHIO’s services and architecture on the requesting side, as well as NYeC’s on the responding side.
Optionality in a scenario also enables actions for which a clear policy or standard has not been established, or other controversial topics, to be considered. For example, in the above scenario, law enforcement administering first aid and accessing an individual’s PHR is included because it was identified as an action in the HITSP emergency responder use case. Including it in the scenario facilitates a discussion about an issue—the clear alignment between policy, the technical standard that provides interoperable access to PHRs, and law enforcement’s willingness and readiness to access PHRs—that appears to be unresolved at this time. As previously stated, this project focused on the medication history and laboratory results use cases, not on the emergency one. Although there will be no discussion of the emergency use case, it is important to point out that a scenario, when constructed this flexibly, can accommodate such a discussion in future studies or when this methodology is applied in the field.

Multidimensional analyses must accommodate alternative actions to surface key findings. In the above scenario, three alternatives provide differing means for accessing health information—two in which the PHR is accessed each by a different actor, and one in which health information is requested from a HIE or the CDO participating in that HIE. Each of these alternatives highlights a different set of access, use, and control issues. For example, since Ms. Doe is unconscious, accessing her PHR would require a break-the-glass action, whereas it would not when accessing Mr. Public’s. Moreover, there may be differences in implications for accessing PHRs because of the differences in actors (EMT versus emergency physician versus other ED personnel).

Even within an alternative action, a scenario can provide further optionality. In Alternatives 1 and 2 above, Mr. Public can provide access to his PHR directly via the USB drive he has on his person (freestanding PHR model) or over the Internet (Web-based or health records bank models). The differences in methods of access and which model is accessed may also differentially affect access, use, and control issues.

**Key Features of the Scenario Used in This Project**

**Pertinent Use Cases**

- Emergency responder, small-scale incident
- Registration and medication history
- Laboratory results

**Constraints Placed on the Optionality in the States and HIEs Involved**

To create realistic targets in the scenario, the following constraints were placed on state 1 and state 2.
State 1

*State 1*, in which the responding HIE resides, has an independent state-level HIE (i.e., not led by state government) formed as a public-private partnership. The state-level HIE has adopted convener and coordinator governance roles but provides no technical services or operations to local HIEs. (For more information on state-level HIE governance and technical roles, see FORE, 2008.)

There are more than 20 local HIEs in the state.\(^2\) *State 1* deploys a two-tier approach in which the state-level HIE (tier 1) supports the local HIEs (tier 2) by creating and deploying common policies, technical standards, and protocols, with local HIEs having the autonomy to develop their own HIE architectures and business models based on their respective clinical and patient priorities.

The local HIEs that are actually exchanging data deploy the IBM prototype architecture. This architecture is noted for the following characteristics (Gartner, 2007):

- The local HIE is composed of a number of “communities” across which HIE services are implemented by previously agreed-to standards.
- Members within a community may interact with each other directly without having to go through the “community hub,” which reduces hub traffic but requires conformance to standards.

---

\(^2\) In reality, only a few of the local HIEs are actually exchanging health information. The rest are in the organizational development or early implementation stage. This scenario is deliberately written as a future state condition to reveal how access, use, and control will be affected by multiple HIEs operating together, which is the whole point of the NHIN.
• The local HIE architecture provides clinical document repositories, which could also be maintained with the community hub. A document locator service combined with a registry tracks individual reports, other clinical documents, and pertinent metadata.

**State 2**

*State 2*, in which the requesting HIE resides, has an independent state-level HIE formed as a public-private partnership. The state-level HIE has adopted convener and coordinator governance roles and provides technical operations for local HIEs. Included in the technical operations are a master person index, a master provider index, a RLS, and a means to standardize clinical data (e.g., translating laboratory test codes to LOINC). The state-level HIE also provides applications for administrative data sharing, eprescribing, patient clinical history, patient medication history, and supplying data to PHR initiatives.

The more than two dozen local HIEs deploy either the CSC or Northrup Grumman prototype architectures. Reconciling different architectures at the local HIE level with the backbone infrastructure and other services of the state-level HIE may cause interesting access, use, and control issues. However, for simplicity, this scenario will focus on the latter architecture, which is noted for the following characteristics (Gartner, 2007):

• A set of core services to the participating CDOs, including patient and provider identification, data location and retrieval, anonymization and relinking, terminology mediation, authorization, authentication, auditing, and the storage and maintenance of patient permissions
• A directory (a registry similar to the Internet’s domain name servers) of CDOs connected to gateways enabling CDOs and their systems to be found when queried
Results

For brevity, not all of the results from the walk-through of the scenario are reported. Instead, three result sets are reported as examples of the types of findings, implications, and recommendations that were uncovered. These examples simultaneously:

- Describe how the factors interact to influence access, use, and control issues
- Suggest practical solutions stemmimg from the findings and implications
- Demonstrate how the walk-through step in the methodology was conducted, which may be illustrative for those interested in using this methodology in the field

These examples are provided with the following caveats:

- Some findings that may seem obvious are not discussed here because they have been reported elsewhere.
- Given the number of permutations that could arise from crossing the variations of each factor with those of all other factors, it was not possible to analyze each permutation in this project. Consequently, there are no findings to report for permutations not analyzed.

Findings, Implications, and Recommendations

<table>
<thead>
<tr>
<th>Example 1</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Factors Affecting…</td>
<td></td>
</tr>
<tr>
<td>• HIE architecture – MPI contamination</td>
<td></td>
</tr>
<tr>
<td>• HIE policies and procedures – DURSA, operational policies and procedures, SLAs</td>
<td></td>
</tr>
<tr>
<td>Access, Use, and Control Issues…</td>
<td></td>
</tr>
<tr>
<td>• Subject and user identity arbitration</td>
<td></td>
</tr>
<tr>
<td>• Availability of access and disclosure information regarding a consumer's PHR and HIE data</td>
<td></td>
</tr>
<tr>
<td>• Routing of consumers' request to correct data</td>
<td></td>
</tr>
<tr>
<td>Encountered in Walk-Through Step</td>
<td></td>
</tr>
<tr>
<td>• Request for patient’s health information reaches the responding HIEs located in state 1</td>
<td></td>
</tr>
<tr>
<td>• Responding HIEs query their respective MPIs and other network services that matches the patient and finds pertinent records</td>
<td></td>
</tr>
<tr>
<td>• Pertinent records are found, but data accuracy is unknown because of MPI contamination</td>
<td></td>
</tr>
</tbody>
</table>

Findings:

- MPIs have a certain level of contamination (error rate due to duplicate data, inaccurate data, missing data, data incorrectly associated with the patient). MPI contamination may cause the responding HIE to send erroneous data to the requesting HIE.
- MPI contamination can occur in each of the nearly two dozen local HIEs operating in state 1.
- Many CDOs also deploy a MPI. Contamination can also occur at the enterprise level MPI. Consequently, CDOs might pass on erroneous data to the local HIE, creating a cascading effect.
- In state 1, in which the responding HIE resides, there are thus two levels in which there can be cascading effects of MPI contamination. If the scenario was switched and state 2 were the responding HIE, then because of its HIE architecture there would be three levels for potential cascading errors to occur owing to MPI contamination (CDO, local HIE, state-level HIE).
- The current draft of the DURSA states that the HIE “warrants and represents that the Data it provides is an accurate reproduction of the data that is contained in its System” (DURSA Section 14.06 Accuracy of Data). This statement is corroborated by the HITSP Interoperability
Specification and draft CCHIT network certification criteria. Some of the data provided by the responding HIE is, in fact, an accurate reproduction of the data in the HIE’s system; it just happens to be erroneous because of MPI contamination.

**Implications:**
- In many instances, it will appear to the requesting HIE, and consequently the clinician who requested the health information, that it has received a valid record. How will the requesting HIE know it has received erroneous data? Will such erroneous data cause a different clinical decision to be made?
- If the requesting HIE suspects or ascertains that it has received erroneous data, does the requesting HIE have any responsibility to inform the responding HIE of such? Does the responding HIE have any responsibility to acknowledge the receipt of this information and take action to correct it?
- Although it may be a best practice, does the responding HIE have any responsibility to monitor and maintain the data quality of its MPI at levels agreed upon in a DURSA among HIEs or a SLA between it and participating CDOs?
- If a responding HIE repeatedly sends erroneous data to requesting HIEs to a degree deemed to be intolerable (yet to be determined), does that constitute a breach under the DURSA?
- On the back end, the patient reviewing an access-and-disclosure report could discover that erroneous data were provided to the requesting HIE, triggering a consumer request to correct data, and causing both the requesting and the responding HIEs to expend additional effort to do so.

**Recommendations:**
- HIEs should institute a formal process to monitor, maintain, and measure the data quality of their MPIs and other systems.
- HIE contracts with participating CDOs should contain an article stating that CDOs will make every attempt to maintain data quality in their respective MPIs and source systems.
- The DURSA should contain an article of agreement whereby the requesting HIE notifies responding HIEs that it has received erroneous information, when known.
- The DURSA should contain an article of agreement whereby the responding HIE accepts and responds to notifications from requesting HIEs that the latter has received erroneous information.
- HIEs should measure, among other things, the percentage of consumer requests to correct data stemming from poor data quality in their MPIs and other components of their systems.

In states where they exist, state-level HIEs are in an excellent position to coordinate the above actions.

**Example 2**

<table>
<thead>
<tr>
<th>Factors Affecting…</th>
<th>Access, Use, and Control Issues…</th>
<th>Findings:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy, federal and state law</td>
<td>Management of consumer choices to not participate in the network</td>
<td>Request for patient’s health information reaches the responding HIEs located in state 1</td>
</tr>
<tr>
<td>Technical standard</td>
<td></td>
<td>Responding HIEs query their respective MPIs and other network services</td>
</tr>
<tr>
<td>HIE architecture – error in the network at the HIE or CDO level</td>
<td></td>
<td>that matches the patient and finds pertinent records</td>
</tr>
<tr>
<td>State-level HIE role</td>
<td></td>
<td>Permissions services discloses that the individual has chosen not to participate in the network</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
It is not clear from current documentation whether responding HIEs will reply to the requesting HIE with a message that there is no health information to return because the consumer has elected not to participate in the network. Without such a message, the requesting HIE may not know there was no returned health information because there is:

- No actual health information to transfer
- No health information to transfer because the consumer has elected not to participate, but valid health information truly exists at one or more CDOs participating in the HIE, and might be obtained directly from the provider
- Some other error in the network that might be an artifact of the HIE architecture (e.g., the responding HIE deploys a central repository and the repository incorrectly associated no pertinent health information to the consumer)
- An error at the CDO level (e.g., the CDO incorrectly associated no health information to the consumer and passed that on to the HIE) causing the HIE to reply with a "no health information to return" message
- A state law that prohibits sending health information that happens to be that which is specifically requested
- The HITSP consent directive appears to provide the ability to capture the consumer’s choice to participate or not in the network, although it is not clear whether this has ever been attempted.

Implications:
- Without a message in the reply from responding HIEs stating that the consumer opted out of the network is the reason there is no health information to return, providers from the requesting HIE may react in a variety of ways, including:
  - The provider may make a clinical decision based on no health information, which is often the case today. But how acceptable is that situation as the NHIN continues to develop? If the clinician consistently receives no health information without an accompanying explanation, the clinician may discontinue using the HIE. This action may mean that the improved quality of care and cost-reduction benefits of HIE will not be achieved to the extent desired by the industry. It could also result in fewer transactions between HIEs, which could be detrimental to the business model of a HIE.
  - The provider may not be aware that health information actually exists at the CDO level and that it can be accessed directly from CDOs, should the consumer feel more comfortable with provider-to-provider communication (the current pre-NHIN model) and gives his or her consent.
- Since there can be different reasons for which there is no health information to return to a requesting HIE, replies should contain an explanatory message informing them of the specific reason for that transaction, as well as what alternate actions the requesting HIE can take to obtain the sought-after information in a timely manner. There may need to be an article in the DURSA among the HIEs, as well as an article between the local HIEs and their participating CDOs, to implement this transaction.
- Differences in state-level HIE governance and technical operations structures may require different ways to accomplish replies to requesting HIEs containing explanatory messages. In state 1 where technical operations are not provided, the state-level HIE may need to collaborate with the local HIEs so that they all implement this transaction uniformly. However, that collaboration may be only part of the effort required if the roles were switched and state 2 were the responding HIE. State 2 may still need to collaborate with the local HIEs to obtain agreement regarding the standard way to implement this transaction, but then it must also implement that transaction in the technical operations it provides. Note that only two variations surfaced because of the constraints placed on the scenario (i.e., the characteristics of the state-level HIE governance and technical operations structures). There are undoubtedly other variations given the possible permutations when different governance and technical operations structures are inserted in the state variables.
- Although the issue regarding whether the HITSP consent directive can capture the consumer’s
choice to participate or not in the network must still be addressed, the salient point here is not whether the consent directive can capture that choice but whether it can communicate that choice to requesting HIEs.

**Recommendations:**
- HIEs, including state-level HIEs, should include statements in replies to requesting HIEs that explain the reasons why there is “no health information to return”.
- HIEs should develop the necessary articles for the DURSA among HIEs, the SLA between the HIE and participating CDOs, and their respective operational policies and procedures that commit the entities to communicating reasons for “no health information to return” replies. In states where they exist, convening and coordinating state-level HIEs are in an excellent position to negotiate these articles with local HIEs and CDOs.

In states where they exist, state-level HIEs are in an excellent position to coordinate the above actions.

**Example 3**

<table>
<thead>
<tr>
<th>Factors Affecting…</th>
<th>Technical standards</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>HIE architecture</td>
</tr>
<tr>
<td></td>
<td>State-level HIE role</td>
</tr>
<tr>
<td></td>
<td>State law</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Access, Use, and Control Issues…</th>
<th>Access management – assigning access privileges</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Routing of consumer requests to correct data</td>
</tr>
</tbody>
</table>

**Encountered in Walk-Through Step**
- Request for patient’s health information reaches the responding HIEs located in state 1
- Responding HIEs query their respective MPIs and other network services that matches the patient and finds pertinent records
- Permissions services discloses that the individual has chosen to participate in the network
- Consent directives are accessed to determine if the patient has consented

**Findings:**
- Consent directives can be implemented by multiple entities (CDOs, local HIEs, state-level HIEs with technical operations). HITSP documentation states that if there is a conflict among consent directives, the entities are encouraged to detect and resolve them according to existing policy.
- Consent directives may actually benefit states that have stricter laws than HIPAA in some ways. For example, state 1 requires a patient’s written consent before the release of most health information, even for treatment, payment, or operations (TPO), which can be implemented by a onetime general consent signed by all new patients. That type of consent in turn may be implemented in a consent directive for HIE purposes.

**Implications:**
- Consumers may have a consent directive across multiple entities (CDOs, local HIEs, state-level HIEs with technical operations). Some of these consent directives may be out-of-date, may contradict other consent directives, or may contradict the consents the consumer has been managing in his or her PHR. Further, the consumer may not recall which entities are managing a consent directive for him or her at any given time and thus may not know that a consent directive needs to be updated or terminated and which entity to approach to do so.
- Such entities will spend a certain level of effort coordinating the consent directives across entities, as well as managing those they have on file for the individual.
- A responding HIE may release health information because it faithfully followed the consent directives on file for the individual. Nevertheless, conflicting consent directives across CDOs, local HIEs, and state-level HIEs may cause an entity to release health information that is not in accordance with what the individual believes are his or her most recent consents. In addition to
causing confusion for both the consumer and the entities, this situation could trigger a consumer request to update or terminate one or more consent directives. Although not the same as consumers requesting corrections to health information, the effort to make such corrections may be the same. This back-end effort may be avoidable to a degree if entities minimize conflicts among consent directives on the front end.

- If consents are implemented through consent directives (or through the HIE’s permissions services) in states in which their laws are stricter than HIPAA, then the health information exchange process can continue. However, if no electronic version of the consent is available, the HIE process may be halted at this point until there is confirmation that a paper-based consent has been signed by the patient, the patient has provided oral consent, or the entities involved believe there is implied legal consent. Moreover, managing conflicting consent directives across local HIEs and CDOs would still be an issue.

**Recommendations:**
- CDOs, local HIEs, and state-level HIEs with technical operations should institute
  - A strategy that keeps the number of consent directives a patient may have to a minimum
  - Measures that monitor and synchronizes consent directives across the entities

In states where they exist, state-level HIEs are in an excellent position to coordinate the above actions.
Conclusions

Conclusions and General Principles

A number of conclusions and general principles can be gleaned from the above findings, implications, and recommendations.

Methodology Proven Useful

Whereas previous analyses and projects identified higher level policy-related findings, this project found a sufficient number of findings, implications, and recommendations at a deeper, operational level. Thus, the target of adding value to previous works was met. Moreover, the flexible methodology was adept at uncovering findings, and it can be used in the field and in future studies.

Results Were Found in the Expected Areas

After the walk-through process, most of the findings and implications were discovered in the actions before and after requesting and receiving registration and medication history data, as well as laboratory results. This outcome stands to reason. If access, use, and control were thought of a set of components, the access component encompasses the actions before requesting and receiving health information—registration summary, medication history, and laboratory results in this instance. It is in this component where credentialing, authorization, and authentication of the provider, and the consents provided by the individual, take place. Consequently, access issues will naturally surface when attempts are made to match patients to their records and access their health information. As the above examples illustrate, a number of such issues manifest themselves in this component.

By the time registration summary, medication history, and laboratory results are accessed, the necessary credentialing, authorization, and authentication would have already been provided. Further, the patient would have given his or her consent for the provider to use the health information. Thus, there would be fewer access, use, and control issues raised at this point.

Some access, use, and control issues, such as consumers requesting corrections to data, surface both before and after registration summary, medication history, and laboratory results have been accessed. The paragraphs below describe these issues in more detail.

Tighter Front-End Controls May Save Effort on Back-End Processes

The examples point out a not surprising, but a very important, point nonetheless: actions on the front end can trigger control issues on the back end. For instance, in Example 1 above, poor data quality in MPIs on the front end could result in a consumer request to correct data on the back end. In actuality, better data quality extends well beyond this example and could be pertinent in all other areas where consumers can review the access and disclosure of their personal health information. Therefore, data quality on the front end—from CDO to counterpart HIE systems, repositories, and MPIs—is a key factor for success.

In Example 3 above, lack of coordination in managing consent directives across all entities involved in HIE on the front end could similarly result in a consumer request to update or terminate one or more consent directives. These two examples underscore the point that tighter controls on the front
end may save time and resources on the back end. In addition, front-end controls may enhance the perceptions of clinicians and consumers about the quality of operations conducted by HIEs.

**Findings, Implications, and Recommendations Generate a Valuable Discussion**

Perhaps equally as valuable as the findings, implications, and recommendations is the discussion they generate during the walk-through analysis and after the results have been identified. Take the discussion that can be generated from the consent directives issues in Example 3. In the scenario, state 1 has a law to which the responding HIE must comply that requires patients to provide written consent even for TPO. Capturing a general consent on a onetime basis for all new patients satisfies this requirement. This general consent could be implemented as a consent directive. Thus, when the responding HIE references the consent repository and finds the consent directive, the responding HIE can send the requested information.

However, what happens when the general consent is not electronically available? If a written consent is not available, the law allows for the release of health information if the patient gives oral consent or there is implied consent. If the patient being treated in state 2 provides oral consent, or even if there is implied consent, how does either type of consent get communicated electronically from the requesting HIE to the responding HIE? Since state laws such as this are not the norm, most actors, from providers to software developers, may not be aware of this law. Would the emergency physician, thinking this encounter is covered under TPO, know to obtain oral consent? Is the functionality prevalent enough in EHR and HIE systems to capture the oral consent and contain it in the request to the responding HIE? If oral or implied consent is not contained in the electronic request, what does the responding HIE document as the type of consent upon which it released the patient’s health information?

As the project team found, this type of discussion came up regularly. Similar discussions in the field can engage multiple stakeholders and enable them to focus their efforts on identifying a practical solution.

**Recommendations for Future Action**

Given the usefulness of the methodology and value of the findings, the following actions are recommended:

- The findings, implications, and recommendations and the methodology should be distributed to the NHIN contractors so that they can factor them into their trial implementations.
- There is much synergy between the state-level HIE and the NHIN trial implementers. There is an opportunity to take advantage of the leverage that can be obtained through collaborative efforts. The state-level HIEs and the NHIN trial implementers should plan on ways to collaborate with each other.
- Given the time and resource constraints of this project, many of the ways in which the factors interacted with the six areas of access, use, and control were not analyzed. Further funding should be provided to continue this effort.
References


www.staterhio.org/documents/SLHIE_report_final_draft_10_16_07_print_final.pdf
http://staterhio.org/documents/Final_Report_HHSP23320074100EC_031007_000.pdf
HITSP (Health Information Technology Standards Panel).
(Members only area).
www.hhs.gov/healthit/usecases/documents/EHRLabUseCase.pdf
## Access Management

<table>
<thead>
<tr>
<th>Question</th>
</tr>
</thead>
<tbody>
<tr>
<td>What is the model for the HIE? RLS, data repository, data mirror, other?</td>
</tr>
<tr>
<td>Given its purpose, mission, and data-sharing model, is the required information available from or through the HIE?</td>
</tr>
<tr>
<td>Who controls access privileges and how?</td>
</tr>
<tr>
<td>What data use agreements must be executed prior to accessing information?</td>
</tr>
<tr>
<td>Who can access the data and for what purposes?</td>
</tr>
<tr>
<td>What uses and groups are barred from accessing the information?</td>
</tr>
<tr>
<td>What are the provisions for emergency access?</td>
</tr>
<tr>
<td>What legal jurisdictions, laws, and regulations are applicable?</td>
</tr>
<tr>
<td>What user training or education, if any, is required prior to first access?</td>
</tr>
<tr>
<td>What type of user support will be provided?</td>
</tr>
<tr>
<td>Under what circumstances will user access be suspended or terminated?</td>
</tr>
</tbody>
</table>

## Entity Authentication

<table>
<thead>
<tr>
<th>Question</th>
</tr>
</thead>
<tbody>
<tr>
<td>How is identity-proofing managed and performed?</td>
</tr>
<tr>
<td>Who provides and manages user credentials, including medical credentials?</td>
</tr>
<tr>
<td>How is nonrepudiation ensured?</td>
</tr>
</tbody>
</table>

## Subject and User Identity Arbitration (Patient Data Matching)

<table>
<thead>
<tr>
<th>Question</th>
</tr>
</thead>
<tbody>
<tr>
<td>How will a correct patient match be determined?</td>
</tr>
<tr>
<td>What patient identity data are used to connect patient records across the various participating organizations?</td>
</tr>
<tr>
<td>What confidence level is necessary to positively identify a patient?</td>
</tr>
<tr>
<td>What record-linking algorithms will be used?</td>
</tr>
<tr>
<td>How are these algorithms tested and validated?</td>
</tr>
<tr>
<td>Are there different confidence levels for different uses of the information?</td>
</tr>
<tr>
<td>How are duplicates, overlays, and merges handled by the HIE?</td>
</tr>
<tr>
<td>Is there an error-handling process for managing new records added to the database?</td>
</tr>
<tr>
<td>What is the contamination rate of each contributor to the HIE?</td>
</tr>
<tr>
<td>What are the data quality standards that must be met prior to acceptance of new data?</td>
</tr>
<tr>
<td>How is compliance with data quality standards assessed and validated?</td>
</tr>
<tr>
<td>How is accountability for compliance with data quality standards managed and enforced?</td>
</tr>
<tr>
<td>How is the relationship of the requestor to the patient established?</td>
</tr>
<tr>
<td>How does authorization occur if subject permissions are not specified?</td>
</tr>
<tr>
<td>How is “break the glass” audited across HIEs?</td>
</tr>
<tr>
<td><strong>Routing of Consumer Requests to Correct Data (Information Management)</strong></td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>What is the process for patients requesting changes to their records?</td>
</tr>
<tr>
<td>Are disclosure logs provided to patients upon request?</td>
</tr>
<tr>
<td>What role will patients play in ensuring the accurate identification of their records and the clinical data accuracy of the information contained therein?</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Access and disclosure information regarding a consumer’s PHR and HIE availability</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Are exchanges between consumer PHR and the HIE audited?</td>
</tr>
<tr>
<td>How will disclosures from the exchange be tracked and reported?</td>
</tr>
<tr>
<td>How are disclosures from a remote HIE captured to the PHR?</td>
</tr>
<tr>
<td>How is the purpose for inquiries to the HIE or a PHR captured so that they can be added to a disclosure log?</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Management of Consumer Choice (Patient Consent)</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>How are patients notified about the HIE and their participation options?</td>
</tr>
<tr>
<td>How does the HIE manage patient consent and permissions?</td>
</tr>
<tr>
<td>Are individuals able to request restrictions on disclosure of their records?</td>
</tr>
<tr>
<td>How are providers who are requesting information notified when an individual has opted out or chosen not to have his or her information in the HIE?</td>
</tr>
<tr>
<td>How is information required for uses such as public health reporting and biosurveillance managed when the individual opts out?</td>
</tr>
<tr>
<td>Who will notify patients if there is a privacy breach in the HIE?</td>
</tr>
</tbody>
</table>