**Florida Health Information Network**

**Architectural Considerations for State Infrastructure**

# Draft White Paper

*Prepared for the Governor's Health Information Infrastructure Advisory Board*

This White Paper represents a consensus of the views of its authors and the product of their research. It does not necessarily represent the individual views of any author or any author's employer, or of the State of Florida.

Version 6.2 – Last update April 19, 2007

**Florida Health Information Network**

**Architectural Considerations for State Infrastructure**

# Executive Summary

## Background

Health policy literature is saturated with evidence that health information technology, appropriately deployed in the health care delivery system, can have a dramatic effect on the effectiveness of the US system. Several reports by federal agencies have also highlighted the importance of the role that technology can play in improving healthcare. Why is health information being looked at as a tool to create a better health care system? And what part of the health care delivery system needs to be fixed? It is now common knowledge that our health care system is often unsafe and inefficient. More people have a chance of dying from a preventable medical error than from an auto accident, breast cancer or AIDS. At the center of this health policy debate is the notable study, published in 1999, by the Institute of Medicine's (IOM) Committee on the Quality of Care in America. The frightening statistic demonstrated that between 44,000 and 98,000 hospital deaths each year are related to preventable medical errors.

A follow-up report released by the IOM in 2001 identified the use of IT as a means for transforming healthcare, not only addressing the issue of preventable medical errors and other patient safety issues, but also the ballooning costs of healthcare in America. "Safety, Achieving a New Standard of Care", released by the IOM in November of 2003, continues to emphasize technology and patient safety. The report focuses on patient safety and healthcare quality.

The growing evidence of a failing health care system coupled with double digit increases in health care cost growth, prompted health policy makers of Florida to take a proactive health care reform position through strong legislative and executive order directives.

On May 4, 2004, Governor Jeb Bush signed Executive Order Number 04-93 as he envisioned a safer, more effective health care delivery system for the citizens of Florida through the deployment of information technology. He recognized the need for state leadership in the area of creating a health information infrastructure.[1] With the executive order, the Governor established the Governor's Health Information Infrastructure Advisory Board (GHIIAB) pulling together thought leaders in health information technology, public health, health policy, and health care practitioners and charged this expert group with advising and supporting the State and the Florida Agency for Healthcare Administration (AHCA) as it creates a plan to promote the development and implementation of a Florida HIT infrastructure.

*The 2004 Affordable Health Care for Floridians Act,* Chapter Law, 2004-297, directs the Agency to "develop and implement a strategy for the adoption and use of electronic health records." The Florida Center for Health Information and Policy Analysis was further directed by the Legislature in 2006 to develop an electronic health information network for the sharing of

[1] Governor's Health Information Infrastructure Advisory Board and Florida Agency for Health Care Administration, *First Interim Report to Governor Jeb Bush*, February 2005.

electronic health records, pursuant to s. 408.062,(5), F.S. The Agency has worked toward this latter responsibility by working with the Governor's Health Information Infrastructure Advisory Board to promote the development of health information exchanges.

Furthermore, the Legislature provided $2 million in funding for the Florida Health Information Network Grants Program in FY 2006-2007 and $1.5 million in FY 2005-2006. Funding this program has spurred local communities to develop local health information exchanges by drawing on donations, volunteers, and grant funding. Groups of stakeholders interested in developing health information exchange have formed organizations called Regional Health Information Organizations (RHIOs) representing many health care stakeholders including providers, employers, insurers, community groups, public health officials and State Universities. Although in the initial phases of development, three RHIOs (Big Bend RHIO, Palm Beach Community Health Care Alliance, and Tampa Bay RHIO) are currently operating networks that can be accessed by hospitals and physicians participating in the RHIO. An additional four organizations have received FHIN grants and these RHIOs will begin to exchange data in 2007.

The development of the Florida Health Information Network (FHIN) is an undertaking driven by the GHIIAB and AHCA and supported by the health care stakeholders of Florida.. The initiative proposes an Internet-based, statewide network that will integrate communications and data transfer among local health information networks (HINs) and RHIOs, establish standards for health information exchange and promote health information exchange among authorized health care providers. The FHIN will maintain a state-level server that functions as the highest level server in a statewide client/server hierarchy. The FHIN will make data communications among Regional Health Information Organizations RHIOs and HINs more efficient and timely and increase the effectiveness of health information exchange on a statewide basis.

<u>The FHIN Will Facilitate Communications and Data Queries Among RHIOs</u>

- The FHIN will perform a necessary function as a central communication link in the state for health information exchange. The FHIN will be responsible for providing access for authorized users to clinical data stored in databases across the state.
- The FHIN will maintain an Enterprise Master Patient Index (EMPI) of all patients receiving medical care.
- The FHIN server will also operate a RLS that will use the listing of patient identifiers contained in the EMPI to query health care providers in each RHIO or HIN in order to collect the appropriate patient records.

<u>The FHIN Will Take the Lead in Specifying Technical Standards</u>

- The FHIN will be the state's lead authority in establishing and maintaining technical standards among the RHIOs and HINs for data communication, data queries, the MPI/RLS, web services and other areas where networks need to employ identical technical specifications to connect to the FHIN.
- The FHIN will specify standards for authenticating users to determine if they are authorized to access patient records, and to authorize RHIOs that wish to connect to the FHIN.

The FHIN Will Provide a Portal for Other Databases

- The FHIN server will function as the major portal for integrating state agency health care datasets and making them available to authorized users. It will establish and maintain the levels of security, confidentiality and certification of users that match the high levels of security required for all patient records.
- The FHIN server can provide access to state agency datasets that are already available electronically, such as:
    - The State Health Online Tracking System (SHOTS) immunization data from the Department of Health (DOH).
    - The Vital Statistics and Cancer Registry data held by the DOH
    - Medicaid data from the Agency for Health Care Administration (AHCA).
    - Inpatient and outpatient data held by the Florida Center for Health Information and Policy Analysis at AHCA
    - The U.S. Department of Defense and the Veteran's Administration
    - Payers, such as Availity.

**The Provider's Perspective of Health Information Exchange**

The discussion of the FHIN begins with the relationship between the provider's needs for patient records and the technical architecture of the FHIN and local RHIOs. The clinical point-of-care is the basic functional orientation of the FHIN, which is designed to support medical decision-making by providing the most complete information about a patient, when needed and when requested.

Provider's Workflow As It Relates to the FHIN

- The way in which the technical specifications of the FHIN server fit the clinical workflow could determine how well the FHIN is accepted by providers. Each step of the clinical workflow has a technical counterpart in the FHIN.

Minimal Clinical Dataset Recommended for the FHIN

- A workgroup was set up on behalf of the GHIIAB to define a Minimal Clinical Dataset that should be stored on each RHIO server. While a key driver for defining this subset of records remains user adoption, it should be noted that standardization on a set of fields also enhances the aim of interoperability, as it ensures that a consistent data set can be exchanged between RHIOs.
- Data fields for the Minimal Clinical Dataset include:
    - Demographic information
    - Provider information

- Problem list of ICD-9 codes
- Orders
- Lab reports
- Allergies
- Adult and Pediatric Immunization Status
- Pediatric Vital Statistics – Collected Up to 18 months

**The Role of the RHIO in the Florida Health Information Network**

The RHIOs and other health information exchanges play an important role as community "umbrella" organizations that bring health care stakeholders together and as network intermediaries between the providers in the local community and the FHIN. The RHIOs take on the responsibility of bringing providers together for the purpose of sharing health care data and integrating their disparate computer systems into a health care data network that can pass medical records among all participants. While the FHIN will provide statewide connectivity, the RHIOs are responsible for working at the local level with providers, laboratories, radiology labs, clinics and administrators at all levels.

- In 2005 three not-for-profit corporations organized as RHIOs received FHIN grants to develop health information exchanges.
- In 2006, seven RHIOs were funded under the FHIN Grants Program.

**Building the Florida Health Information Network**

The FHIN is envisioned as a statewide health information infrastructure that will enable health care professionals to access a patient's medical records from any provider database connected to the network over a secure Internet connection.

- The FHIN represents a collaborative effort between the public and private sectors, state and local governments, RHIOs and health information exchanges, providers, employers, consumers, health plans and payors.
- The FHIN proposes to interconnect health care providers across Florida to facilitate the sharing of health care data without regard to where in the state the consumer resides or where the health care was delivered.
- The FHIN infrastructure will be built around a central server that will maintain connectivity among RHIOs or other health information networks in the state.

**Technical and Non-Technical Issues Facing the Florida Health Information Network**

<u>RHIO Architecture on a Sliding Scale</u>

This section discusses a sliding model which can be used to understand the differences between the centralized and decentralized database structures, which will in turn be used to build the framework for a mixed-mode architecture. It is noted that in each of the four models along a sliding scale from centralized to decentralized (and any other potential variations that may arise) there is a duplication of data in the central repository and in the edge and host servers. In addition to this, if providers of data will not permit direct access to their clinical systems, even a decentralized model will end up with a duplication of data, as the providers will have the expense of providing edge servers.

- After considering the relative advantages and disadvantages of both centralized and decentralized models, an argument can be made for the adoption of a mixed-mode model, which contains the core clinical information most frequently identified by clinicians as being the data they would wish to have displayed in a structured data interface for ease of use.

- The mixed-mode architecture would call for a subset of clinical records defined in a harmonized Continuity of Care Record (CCR) and Clinical Data Architecture (CDA) standard.

- At the end of each clinical encounter the provider would update the patient's health care record based on the latest encounter, and that data would be used to update the central harmonized CCR/CDA.

Authorization and Authentication of End Users

- The FHIN Network Security Workgroup has recommended that each RHIO credential and authenticate clinicians against the Department of Health physician licensing database to ensure that the clinician (or person authorized by the clinician) is credentialed in the State of Florida.

- A trust relationship between servers exists when one server requests information from another, and the requested server does not need to authenticate the individual user request because a trust relationship exists between the two servers. The FHIN Network Security Workgroup endorsed the concept of trust relationships between the RHIOs and the FHIN server.

- The HIPAA Business Associates Agreement (45 CFR §160.103, 164.502(e)(1) and 164.504(e)(1)) is an acceptable mechanism for sharing of data with the RHIO, based on the assumption that the collocation services provided by the RHIO are business functions that could not be performed by the individual entity itself.

- In order to deal with a Business Associate Agreement between the provider and RHIO only, a trust relationship needs to be set up between RHIOs. The recommended trust model assumes that any clinician who has access to data from one RHIO, would automatically have access to patient data for any patient for whom they have been previously authenticated and authorized by any other RHIO.

- It is in the interest of the FHIN to maintain an audit trail of all data requests among RHIOs, in addition to the logging made by the RHIOs themselves.

- Within the model being proposed in Florida, the FHIN would play a crucial role in the authentication process, ensuring that all data shared meet with HIPAA requirements and state statutes.

- As the FHIN sets the cornerstone for an interoperable world of sharing PHI via the Internet to an array of RHIOs around the state, it is critical that security features, functions, audit trails, identity management and non-repudiation controls are an integral part of this process.

Development of a Master Patient Index and Record Locator Service

The Master Patient Index (MPI) is a software program that collects identifying data on patients for the purpose of accurately flagging discrete patient records for an individual patient. Each RHIO will maintain an MPI for patients seen by providers in the local community area;

The Record Locator Service (RLS) holds information on where patient records are located. The RLS identifies records without requiring their central storage, storing just enough information to be able to tie a clinical record to an MPI record, as well as the information about where that record is stored.

- The FHIN Enterprise MPI will mirror all of the RHIO MPIs in a statewide registry that will be updated on a regular basis.

The FHIN RLS will support the non-repudiation of records, providing an authentication mechanism, such as a digital signature, that allows one to verify the data records that were sent from a provider. Although medical care is delivered on the basis of the information presented to the provider, in most models that collection of data is not permanently stored. If, based on an incorrect match of identifiers, the collated record were to provide inaccurate information which resulted in harm to the patient, giving rise to legal consequences, there would be great interest in reconstructing the collated record that formed the basis of the diagnosis. This remains the single most difficult technical challenge for RHIOs.

1. The FHIN Network Security Workgroup recommended that transaction audits for non-repudiation will be conducted at both FHIN and RHIO levels, based on HIPAA and other industry standards.

Privacy and Confidentiality of Patient Records

At the outset the FHIN needs to design the mechanisms to allow for effective and cost-effective patient control of medical information. The fundamental difference between privacy and confidentiality lies in the focus of the data being dealt with. Medical privacy is about the human desire to control what information is shared about a person's health status; confidentiality is about how the danger is handled once the patient and the person holding the data enter into an agreement to ensure that the data are only provided in an appropriate manner to those persons with the authorization to view the data.

- Under HIPAA, there are preexisting conditions under which data may be shared between business entities, normally covered under what is called a business associates agreement (BAA).

- Where a BAA does exist between two entities, explicit patient consent is not required to share data if it can be shown that a valid business function is being performed by the organization receiving data behalf of the provider.
- While fully recognizing patients' rights to be able to control their own clinical information, the authors of this paper would caution against the adoption of opt-out models for RHIOs.
- The authors of this paper would recommend that consideration be given to alternative systems to ensure patient rights, such as the adoption of a personal identification number (PIN) model external to both the source systems and the RHIO.

**Recommendations**

Central Authority for Technical Standards

- The state of Florida should endorse and create an independent, neutral, central, not-for-profit organization to set standards and certify RHIOs to meet the FHIN policy and technical requirements.
- The FHIN will extend web services and content standards to provide state-level reliability and security specifications, and to model the key inter-RHIO processes for health care. The FHIN will work closely with standards recommendations of the AHIC and the NHIN.

Network Security

- Clinicians shall connect to the RHIOs, and RHIOs shall connect to the FHIN using a secure and encrypted communication channel that meets standards as articulated in the HIPAA Security Rule and consistent with provisions in state statutes and other standards bodies.
- Detailed logging of all requests to the FHIN server, or between RHIOs and other entities must be kept at all times, preferably both by the requesting entity and by the requested entity.

Authentication of Users

- The state server shall act as a broker of all transactions among individual entities such as RHIOS, state agency databases or other sources of health care information.
- The FHIN is responsible for credentialing all physicians who want to join a RHIO, or connect directly to the FHIN. Additionally, authentication takes place at the FHIN (credential check) and then the RHIO. Once the user is authenticated at both levels, then all transactions are trusted after FHIN authentication.
- Authentication of clinicians entails the use of digital signatures in two factor authentication and Role-based authentication.

Patient Consent

- It is recommended that a statewide patient authorization system be investigated, possibly using a patient controlled PIN which is externalized to the RHIOs or source systems. This will allow the patient to control exactly who has access to their identifiable health information, while requiring minimum changes to existing systems.

Master Patient Index

- A common set of fields should be identified and used by all RHIOs for patient identification. These should include first and last names, phone number, date of birth, city or location of birth, or a personal identification number (PIN).

Minimal Clinical Dataset

- Each RHIO should create a minimal clinical dataset of priority data fields culled from patient records, to be held on the RHIO server for immediate downloading to the local physician upon request.

**Acknowledgements**

The Agency for Health Care Administration and the Governor's Health Information Infrastructure Advisory Board expresses it sincere gratitude for the volunteer assistance, time and effort of the many individuals and organizations that contributed to the writing of this White Paper.

Questions or concerns regarding this report should be directed to:

Lisa Rawlins, Bureau Chief

Florida Center for Health Information and Policy Analysis

Florida Agency for Health Care Administration

2727 Mahan Drive, MS #16

Tallahassee, FL 32301

Email: RawlinsL@ahca.myflorida.com

Telephone: 850.922-7036

**Florida Health Information Network**
**Architectural Considerations for State Infrastructure**

# Table of Contents

## I. Background and Need for a Florida Health Information Network

Health policy literature is saturated with evidence that health information technology, appropriately deployed in the health care delivery system, can have a dramatic effect on the effectiveness of the US system. Several reports by federal agencies have also highlighted the importance of the role that technology can play in improving healthcare. Why is health information being looked at as a tool to create a better health care system? And what needs to be fix? It is now common knowledge that our health care system is often unsafe and inefficient. More people have a chance of dieing from a medical error than from an auto accident, breast cancer or AIDS. At the center of this health policy debate is the notable study , published in 1999, by the Institute of Medicine's (IOM) Committee on the Quality of Care in America. The frightening statistic demonstrated that between 44,000 and 98,000 hospital deaths each year are related to preventable medical errors. By another count, approximately 1.14 million total patient safety incidents occurred among the 37 million hospitalizations in the Medicare population from 2000 to 2002. Approximately 7,000 deaths each year are attributed to medication errors, with a potential cost in excess of $2 billion in terms of lost income, lost household production, disability, and healthcare expenditures. To treat the effects of these errors, individual hospitals might expect to pay as much as $5.6 billion a year.

A follow-up report released by the IOM in 2001 identified the use of IT as a means for transforming healthcare, not only addressing the issue of preventable medical errors and other patient safety issues, but also the ballooning costs of healthcare in America. "Safety, Achieving a New Standard of Care", released by the IOM in November of 2003, continues to emphasize technology and patient safety. The report focuses on patient safety and healthcare quality.

The growing evidence of a failing health care system coupled with double digit increases in health care cost growth, prompted health policy makers of Florida to take a proactive health care reform position through strong legislative and executive order directives.

In August, 2003, Speaker Johnnie Byrd created the Select Committee on Affordable Health Care for Floridians to investigate trends in the heath delivery system, to review the health insurance market trends and to identify new ideas for health care change. This deliberate legislative body met with stakeholders across the state in a series of public meetings through the fall of 2003, and produced a draft final report in January 2004.[2] Among the many proposals for reducing health care costs, several targeted health information technology. One proposal suggested "the promotion of compatible information technology that permits secure, private information sharing throughout health care." This proposal foreshadows the work on technical standards and interoperable systems within the Florida Health Information Network (FHIN) that is the focus of this White Paper.

Two other proposals in the report of the Select Committee were also in line with the activities of the FHIN. The first proposal suggests requiring the "use of technology to create a single medical record that belongs to the patient and families." This implementation of a personal health record is one goal of the FHIN. The second proposal suggests "timely access to health education, health

[2] Florida House of Representatives (2004). Select Committee on Affordable Health Care for Floridians, Draft Final Report. Retrieved on March 10, 2006 from http://www.fdhc.state.fl.us/affordable_health_insurance/house_committee/house_committee.shtml.

production, disease prevention and early intervention services." Through the FHIN grants program, funded by the Legislature, the Tampa Bay Regional Health Information Organization is undertaking a program to use electronic health records to provide early intervention services and disease management for diabetics, children with asthma and adults with prostate cancer.

Also in 2003, Governor Jeb Bush created the Task Force on Access to Affordable Health Insurance, chaired by Lieutenant Governor Toni Jennings and Chief Financial Officer Tom Gallagher. The goals of the task force included identifying factors contributing to the increasing costs of health insurance in Florida, and to provide policy recommendations to improve access to affordable health insurance at affordable cost. The task force held meetings in the fall or 2003 and early winter of 2004, and in February 2004 published a final report, the *Final Report of the Governor's Task Force on Affordable Health Insurance.*[3]

One recommendation of the report was to promote the utilization of electronic health care information through the use of financial incentives. The report cited research detailing the long term cost savings to providers for installing electronic medical record systems, the improvement in the clinical practice for physicians and their positive impact on health care quality. The report recommended supporting electronic health records that would allow for the capture of patient clinical data and facilitate "caregivers and receivers to share medical records and access clinical information." This goal is consistent with the goals of the FHIN.

Finally, the Legislature passed the *2004 Affordable Health Care for Floridians Act*[4] during the 2004 legislative session. This piece of legislation charged the State Center for Health Statistics with two responsibilities in regard to electronic health records. In the first case, it authorized the State Center to study the relationship between physician information systems and hospitals and other facilities, pointing specifically to the "development of physician information systems which are capable of providing data for health care consumers taking into account the amount of resources consumed, including such information at licensed facilities as defined in chapter 395, and the outcomes produced in the delivery of care" (s. 408.062 (1)(g), F.S.)."

Through this wording, the Legislature shows its interest in the impact of electronic health records and electronic medical records in hospitals and other licensed health care facilities, and how electronic health records can bring about positive outcomes in patient care. In other language added to the *2004 Affordable Health Care for Floridians Act* the State Center is directed to "develop and implement a strategy for the adoption and use of electronic health records." The State Center, and the Agency for Health Care Administration, have worked toward this latter responsibility by working with the Governor's Health Information Infrastructure Advisory Board to promote the development of health information networks, and by administering the FHIN Grants Program to leverage local community efforts to engage health care stakeholders to come together to collaborate on health information exchange in the community.

In his Executive Order on April 27, 2004, President George W. Bush called for the widespread implementation of health information technology and the sharing of electronic health information within the next 10 years. President Bush appointed Dr. David Brailer as the first

[3] Office of the Governor (2004). Final Report of the Governor's Task Force on Affordable Health Insurance. Retrieved on March 10, 2006 from http://www.fdhc.state.fl.us/affordable_health_insurance/index.shtml.
[4] Florida Legislature (2004). 2004 Affordable Health Care for Floridians Act (Chapter 2004-297, Laws of Florida). Retrieved on march 21, 2006 from http://election.dos.state.fl.us/laws/04laws/ch_2004-297.pdf.

National Coordinator for Health Information Technology. Dr. Brailer has stated publicly on multiple occasions that the goal of his office is not to force centralized solutions on healthcare stakeholders, but rather to create an environment that will nurture health information sharing organically. Dr. Brailer advocates the formation of regional health information organizations (RHIOs) that would oversee the implementation of local health information networks. Clinically, this would allow providers to have access to, and use of, health information exchanges where the providers can view their patients' cumulative health data, collated from multiple data sources (e.g., hospitals' clinical information systems, provider-generated claims records, or outpatient clinics).

The state of Florida endorses Dr. Brailer's approach, and is actively promoting and supporting the development of RHIOs around the state. However, while RHIOs can improve the accuracy and availability of health care information in local settings, access to medical records must also be available at the state, national, and even international arenas. This is outside the scope and capability of RHIOs, and is more appropriately the role of a state-level network like the Florida Health Information Network. The FHIN will ensure access to secure, accurate medical records across Florida by providing a technical infrastructure which allows authorized health care workers to obtain health care information on patients from all of the RHIOs connected to the FHIN. The FHIN will ensure the data are applicable to the individual being treated, the transit is secure and efficient, and that the receiving provider is authorized to obtain the information. Additionally, the FHIN will provide access to health care data held in state databases.

Within the state of Florida, there is significant interest to work toward a statewide health information network. On May 4, 2004, Governor Jeb Bush signed Executive Order Number 04-93 as a response to the need for state leadership in the area of health information technology (HIT) infrastructure development.[5] As part of the executive order, the Governor established the Governor's Health Information Infrastructure Advisory Board (GHIIAB) under the chairmanship of Michael Heekin, with 12 other members who represent the health care provider community in Florida. The GHIIAB is charged with advising and supporting the Florida Agency for Healthcare Administration (AHCA) as it creates a plan to promote the development and implementation of a Florida HIT infrastructure.

The GHIIAB has extensively collected data on the current status of HIT in Florida and has presented an interim report to the Governor as well as the Florida legislature. In 2005, AHCA obtained state funding for pilot planning and the implementation of local health information exchange projects. Furthermore, it is the state's intention to nurture local exchanges and to foster the early development of an integrated statewide infrastructure to permit local exchanges to interact as a network as soon as each exchange is able. In the aftermath of Hurricanes Katrina and Rita in 2005, the necessity of securing medical data in electronic format, with secure backup, is even more apparent and urgent.

On November 17, 2005, the Governor's Health Information Infrastructure Advisory Board considered grant proposals for RHIO efforts in the State of Florida. In the prior month the Office of the National Coordinator of Health Information Technology (ONC) announced grants for four Nationwide Health Information Network (NHIN) prototype projects, the Commission on System

[5] Governor's Health Information Infrastructure Advisory Board and Florida Agency for Health Care Administration, *First Interim Report to Governor Jeb Bush*, February 2005.

Interoperability released its recommendations to promote nationwide use of health information technology, and the American Health Information Community (AHIC) prepared updates on five areas of national interest for its November 29th meeting. Given the level of activity at the national level in conjunction with the level of activity in the State of Florida, this paper looks at issues around some of the technical issues required at a state level to facilitate national interoperability.

The development of the FHIN is an undertaking driven by the GHIIAB and AHCA. The initiative proposes an Internet-based, statewide network that will integrate communications and data transfer among local health information networks (HINs) and RHIOs, establish standards for health information exchange and promote health information exchange among authorized health care providers. The FHIN will maintain a state-level server that functions as the highest level server in a statewide client/server hierarchy. The FHIN would make data communications among RHIOs and HINs more efficient and timely and increase the effectiveness of health information exchange on a statewide basis.

As Florida's top-tier HIT resource, the FHIN will manage communications, process data requests and responses, maintain an Enterprise Master Patient Index and Record Locator Service to locate health care records, provide accessibility to independent health care databases and other HINs outside of the state, and establish technical standards that ensure interoperability among all state sub-networks. ONC has awarded several significant contracts to establish standards for services such the master patient index and RLS for the NHIN. The FHIN will work closely with ONC to model its network architecture on the standards of the NHIN.

The FHIN Will Facilitate Communications and Data Queries Among RHIOs

The FHIN will perform a necessary function as a central communication link in the state for health information exchange. RHIOs and HINs in Florida will be able to route relevant record requests through the FHIN to the appropriate source electronic medical record (EMR) system or RHIO, and return the appropriate response(s), using HL7, X12 and other communication standards. The FHIN will be responsible for providing access for authorized users to clinical data stored in databases across the state.

As part of its access responsibility, the FHIN must be able to verify, or authenticate, the credentials of users to validate the identity of the user and to verify that he or she is authorized to request data over the network. While each RHIO will be responsible for authorizing local providers, allowing the FHIN to authenticate users for RHIOs in other locales lets regional servers send updates to only one location and reduces the time required for regional servers to retrieve patient records. The FHIN will also be capable of communicating with HINs outside of Florida, either at a state or at a national level. At present there is little electronic health care data to be exchanged, but that will certainly change in the upcoming years. The FHIN will function as a broker through which RHIOs and HINs in Florida can access patient records from every part of a state or country. As a result the FHIN can make access to patient data from these other resources transparent to RHIOs already exchanging such information via the FHIN.

The FHIN will be responsible for querying clinical datasets held by providers within the local RHIOs and HINs connected to the FHIN. The FHIN will need to locate the correct patient records, compile them and return them to the authorized user requesting the information. The

alternative is to require the regional networks to query every other HIN in the state in a peer-to-peer fashion. This is a complicated and inefficient capability which, without the FHIN, would add to the cost, time to implement, and complexity of each and every in-state RHIO. Of course, there could be cases where it is more efficient to use a RHIO portal directly, instead of submitting a request through the FHIN, when a given record is known to exist only within one RHIO, but these cases should be in the minority.

To support its data query function, the FHIN will maintain an Enterprise Master Patient Index (EMPI) of all patients receiving medical care. Developing and maintaining such an index can be complex. It requires a definitive set of patient identifiers to determine that a patient record is correctly pinpointed, with a high degree of certainty. For the EMPI to function correctly it must be updated as new patients enter the health care system, or change their personal information, for example by changing names after marriage. The EMPI must also support an audit trail of name changes and aliases. Rules for updating the EMPI must be established so that there is no lapse in record location. However, deciding whether patient records are updated and corrected by the patient, physician or by clinical staff is best left to the local provider. Each RHIO must use the same group of patient identifiers so that the FHIN EMPI can accurately locate all patient records.

The FHIN server will also operate a RLS that will use the listing of patient identifiers contained in the EMPI to query health care providers in each RHIO or HIN in order to collect the appropriate patient records. The RLS will have to validate the accuracy of patient information with a high degree of certainty before returning the record to the authorized user, and where the certainty is not high the option of users having the ability to accept or reject a record would need to be implemented. The FHIN server will also have to flag possible mismatches or duplicates, and resolve duplicate health care records that may be connected to different patients; RHIO or HINs are then notified that a possible duplicate exists.

Both the EMPI and the RLS is a core piece of the FHIN. These are key issues. It is possible to assume that one just installs and starts up these two functions, but while it is possible to purchase these systems, they may or may not meet all the legal (or even technical) criteria associated with the tasks required. However, providing these two functions very significantly decreases the scope of responsibility and liability of the RHIOs. As a result the EMPI and the RLS are two of the major issues to be addressed by the FHIN and ultimately rolled down to the RHIOs.

While the RLS is searching for patient records across the FHIN, the RHIO and HIN servers can immediately provide a summary set of patient records to the authorized user, based on the most recent, local patient information. The FHIN will establish a minimal clinical dataset of patient records to be located on the RHIO and HIN, based on the harmonized ASTM Continuity of Care Record (CCR) and HL7 Clinical Data Architecture (CDA) standards. This patient information will represent the essential information needed for patient assessment.

The FHIN Will Take the Lead in Specifying Technical Standards

The FHIN will be the state's lead authority in establishing and maintaining technical standards among the RHIOs and HINs for data communication, data queries, the MPI/RLS, web services and other areas where networks need to employ identical technical specifications to connect to the FHIN. Most of the standards specified by the FHIN will be identical to standards set by national standards organizations, and will align with standards for the NHIN established by

ONC. The technical standards specified by the FHIN should include messaging standards such as HL7 and X12, web services specifications, and standards for the storage and access to patient records based on the harmonized CCR/CDA standards. The FHIN must also maintain technical performance standards for its server activity, such as acceptable downtime, speed of communications and responsiveness of the server to data queries. RHIO and HIN servers should be held to these same performance standards. The FHIN should provide a Service Level Agreements to the RHIOs outlining its service commitments.

The FHIN will also need to specify standards for authenticating users to determine if they are authorized to access patient records, and to authorize RHIOs that wish to connect to the FHIN. The FHIN server will also require standards for updating the EMPI by the RHIOs, specifying the update cycle and which fields must be included for the minimum set of identifiers. The FHIN should also develop standards for future billing and accounting of revenue streams for use of the network. As with all technical standards, those specified by the FHIN are subject to change over time. The FHIN server will need to update its technical standards and incorporate these updates into its service level agreements as information technology systems evolve and as new standards come into place for health information exchange.

The FHIN Will Provide a Portal for Other Databases

The FHIN server will function as the major portal for integrating state agency health care datasets and making them available to authorized users. It will establish and maintain the levels of security, confidentiality and certification of users that match the high levels of security required for all patient records.

The FHIN server can provide access to state agency datasets that are already available electronically, such as the State Health Online Tracking System (SHOTS) immunization data from the Department of Health (DOH) or Medicaid data from the Agency for Health Care Administration (AHCA). Access to both of these datasets is constrained by federal law and state statute to ensure confidentiality of the patient records, and the FHIN server must meet those requirements before making records available. Datasets not currently available electronically, such as the inpatient and outpatient data held by AHCA and the vital statistics and cancer registry data held by the DOH can be made available via the FHIN server. Also, patient records held in the county health departments and public health laboratories could be accessed over the FHIN server.

The FHIN server could also provide access to patient records held by the U.S. Department of Veterans Affairs (VA) or state agencies that hold health care information, such as the Department of Education, Department of Corrections, Department of Juvenile Justice and Department of Financial Services, Department of Elder Affairs and Department of Veterans Affairs. The FHIN will need to meet all appropriate privacy and legal access requirements for state and Federal programs and agencies.

The FHIN server can also function as a portal for health care datasets from independent, non-government organizations. These datasets could include claims data from insurance carriers, or records for or records from patients seen at federally qualified health centers or other providers, including patients without health insurance.

The FHIN could serve as the technical model to drive the diffusion of EMRs and integration of electronic health records to physicians across Florida. The FHIN server can act as the standard for building and connecting future HINs and RHIOs. Once a functioning FHIN is in place to demonstrate the value of interoperability of data access among providers, it should generate interest among physicians in connecting to the network.

In the following sections, the discussion of the FHIN begins at the point of care with the provider, addresses the roles of the RHIO and other health care databases, and finally describes the functional characteristics of the FHIN. The electronic data-sharing enabled by the FHIN is ultimately intended to deliver accurate, appropriate and timely medical information to a physician dealing with a patient's health care issues. Providers will have the ability to send data requests to the FHIN for patient records that are stored in database locations accessible to the network. The role of the FHIN is to pull together all pertinent records on a patient from any of its connected databases, and send them to the provider. The FHIN transports this information to the provider and saves an account of the transaction for audit purposes; no patient records are stored by the FHIN.

Three Levels of the FHIN

The next section discusses the role of the regional health information organization and health information exchange, state agency health-related databases and provider-generated claims databases. Each of these entities makes health care data available to the FHIN and to providers, but each one plays a different role within the network of interoperable health care databases. The RHIO is a neutral organization, generally a not-for-profit, that brings health care stakeholders together within a community or geographic location to share health care data. The health information exchange could be a group of providers that agree to share data among themselves, but is not organized to include all stakeholders.

State agencies collectively hold an enormous amount of health care data that could be used to build historical medical profiles on patients (e.g., the ten years of inpatient data held by AHCA). Payors have databases of every claim generated by providers for medical purposes, which could be used to create case histories of patients. Each one of these entities should be accessible to the FHIN and to the individual provider.

The last section addresses the statewide functions and expectations of the FHIN. The FHIN must operate technically at the network level to ensure statewide interoperability, as a policy-making standards body and as a state level RHIO that convenes all health care stakeholders in the state. Each of these roles for the FHIN are discussed in the final section. Issues relating to security, privacy, business agreements and access to health care data are also identified in this section. The issues themselves are discussed in Part III of this paper.

## II. The Provider's Perspective of Health Information Exchange

The discussion of the FHIN begins with the relationship between the provider's needs for patient records and the technical architecture of the FHIN and local RHIOs. The clinical point-of-care is the basic functional orientation of the FHIN, which is designed to support medical decision-making by providing the most complete information about a patient, when needed and when requested. The RHIO represents the local "playing field" for the physician at the point-of-care, providing interconnection with local provider, laboratory, radiology and other clinical databases. The RHIO also provides a connection to the FHIN with its access to other RHIO and state agency or provider-generated claims databases.

The majority of the health care information exchanged by the FHIN will end up in the hands of a provider, as an aid to his or her medical decision-making. Linking the steps of the clinical process to the technical specifications of the FHIN is one way to begin the discussion of the technical decisions that need to be made regarding an interoperable network that will connect physicians' offices with hospitals, labs, pharmacies and other medical providers. The following narrative presents a scenario in which a patient sees a physician and is brought through a potential clinical workflow, based on the suggestions of several physicians. The discussion covers linkages between the clinical workflow and the technical specifications that underlie each of the steps in the process. While this white paper focuses on the technical details of the FHIN, the technical architecture should always be related to the information needs of the provider in treating a patient.

Provider's Workflow As It Relates to the FHIN

In the following scenario a patient is tracked through an idealized visit to a provider's office for a medical visit. The description of the visit is used for the purpose of highlighting those points at which the physician will need to access data from the FHIN and those issues that relate to the requests for data. At each relevant step in the clinical workflow, the connection to FHIN is identified and discussed.

1. A patient comes into the physician's office for a medical visit. Having signed HIPAA consent forms and required paperwork the patient then discloses personal information that allows the provider's staff to query for health information via the FHIN web portal. In the case of the adoption of a PIN model, this would include the patient releasing their PIN to the providers staff to allow access. Most of this information can be provided as part of the existing intake mechanism, so this step should not place an addition burden on the physician staff.

In step one, the patient has given consent and the physician's staff requests specific demographic and personal information from the patient. The patient may be asked to provide date of birth, gender, contact information, social security account number, insurance coverage information with attendant identifier, or other contact information required for the local RHIO Master Patient Index (MPI) and the FHIN EMPI. These data fields are needed to conduct searches of patient listings. In the absence of a standardized unique identifier (e.g., Social Security Number or Insurance ID) the MPI will need to use an aggregated set of indicators to locate patient records. These indicators will need to be specified and standardized across all RHIOs in Florida so that the FHIN server can locate records of patients based on the same data criteria.

Many exchange organizations hope that the health information exchange will also alleviate the redundant intake process that occurs with every clinical engagement. RHIOs could provide patients with a portable technology, such as a smart card or memory stick, that contains their exchange identifier so that the intake process is much smoother and with less redundant work. The American Health Information Community (AHIC) recommends a single electronic health registration for patients.

> *Going to the doctor or hospital often requires filling out multiple forms. These forms collect information such as name, address, insurance, medications, allergies, etc. Then, when an individual requires lab work or other testing, the same information has to be collected again. A single electronic health registration will make it easier for individuals to give their information and for clinicians to use it. Additionally, the consumer could update the information once and share it with all providers immediately as needed.*[6]

2. Armed with the necessary patient information to query the FHIN, the staff will then access the provider's account on the RHIO or on the FHIN. Medical record requests will be sent to the RHIO for local record listings, and to the FHIN for statewide record listings.

Once electronic security measures which are established and enforced by the regional exchange, and if the patient consents, the staff can find out whether the patient has previously been seen by other providers locally or in other parts of the state. The portal will return a list of medical records that are associated with the patient. The list of clinical records can range from a listing of clinical interactions based on a summary of an entire inpatient admission, to just a single laboratory result. Each clinical record on the list should show a weighted probability that the particular record is correctly associated with the patient, with the highest probabilities listed first. Only records that are above a specified weighted probability, determined by the provider, will be presented on the list of possible records associated with the patient.

Step two is the point at which the provider connects to the FHIN, either directly or through the local RHIO. This step assumes some important background criteria. First, the provider must have a computer capable of accessing the Internet. One might take this for granted, or as a necessary pre-condition. Next, the provider must already have applied to the local RHIO, or directly to the FHIN, as an authorized user of the system. Once the provider is certified and granted access to the FHIN with a sign-in name and password, the provider's office will use these to authenticate itself to the RHIO or the FHIN directly. Providers are encouraged to work through a local RHIO, but in the absence of an available health information exchange organization, then access directly to the FHIN will be available for providers.

If the provider is working through the RHIO, then the RHIO must also be authorized to access the FHIN server in order to access medical records across the state. Finally, the provider must have agreed to a HIPAA Business Associate Agreement (BAA) through the local RHIO, that

---

[6] Office of the National Coordinator for Health Information Technology (2006). American Health Information Community Potential Breakthroughs. Retrieved February 22, 2006 from http://www.hhs.gov/healthit/breakthrough.html

allows providers to share data with other health care providers The BAA should address most HIPAA-related concerns with regard to the relationship between the patients and the RHIOs. The only other major concern regarding HIPAA is the encryption of confidential data and the related security countermeasures within the FHIN itself.

3. Working from the refined list of medical records, perhaps with patient oversight, the provider's staff can select those records that are most appropriate for the patient's visit and request that the full records be sent from the FHIN. These records can then be combined into one report.

Steps three refers to record listings that are returned from the local RHIO, which will query local medical records and the FHIN, which will query statewide medical records, based on the assumption that the provider is working through the RHIO. When a provider submits a request for information on a patient through the local RHIO, its server will match the patient identifying information with patient listings in the local MPI to locate the correct patient records. Once the patient identification is verified, the local RHIO server will determine if a minimal clinical data set is held on the patient and will push that data down to the requesting provider. The local RHIO exchange will also collect all local medical records related to the patient from providers who are members of the RHIO, and push that listing of records to the requesting provider.

The local RHIO server will also pass the patient record request, with the patient identifying information, to the FHIN server. The FHIN server will authenticate the RHIO server and authenticate the requesting provider. The FHIN server will then match the patient identifying information with the patient listing in the statewide EMPI to locate the correct patient records. Once the patient is located in the EMPI, the Record Locator Service (RLS) will collect all medical records held in local RHIO servers around the state. In this step the FHIN will have to connect with the remote RHIO, locate the appropriate records in the remote RHIO, collate all of the patient records and push the records to the local RHIO requester. The local RHIO will then push the statewide record listing to the requesting provider.

In this step record listings are sent from the local RHIO to the provider in several sets. The first set of records will be a summary based on a minimal clinical data set stored in the local RHIO, which is recommended by this white paper. All other health care data will be stored in the provider databases. A second set of records should arrive after a short time delay and will list the patient records available to the physician from local providers. A third set of records could arrive after a short time delay and will list the patient records available from other RHIOs around the state, from state agency databases or from provider-generated claims databases. The patient can be enlisted in the selection of correct records, following which the provider will be in a position to select those records that are pertinent to the patient's visit.

4. All of the discrete records that are combined into the medical report will have an audit trail, so that if a record is determined to be inappropriately merged, it can be discretely unmerged.

Merging of records means that a patient record is added to a listing in response to a provider request for patient records. Unmerging refers to the unlinking of a particular, incorrect record from the list of records. This step recommends that the FHIN and the RHIO servers maintain an audit trail that will record which records were presented to the provider, from which source, and which records were selected. The audit record will be essential for any questions that arise

concerning the use of electronic health records and to satisfy HIPAA requirements. A third party entity should oversee random audits. All audits should be consistent with national standards for health information exchange.

5. Once the cumulative record has been established, potentially with patient oversight, the record is listed on the provider's active list patient list.

This step describes the provider's staff selecting records to produce a cumulative patient record for the physician to use. These records can be printed out for the physician or stored in the office electronic medical record system, if one exists. The provider's staff will also be able download and store selected records if the provider has an electronic medical record system in place, the patient's records could be stored in the provider's server for future retrieval. If the provider does not have an electronic medical record system in place, then the provider may only be able to print the records.

6. When the patient is finally seen by the provider, the patient's cumulative records should already be loaded onto the provider's 'active' list, collated and organized in an intuitive manner for the physician's perusal.

This step refer to the final presentation of patient records to the physician. The presentation layer for reporting patient data is outside the scope of the FHIN white paper, but will be an important variable in physician acceptance of an electronic health record (EHR). One aspect of the presentation of patient records is the potential for linking to the provider's in-house EHR system. The FHIN would make it possible to store selected patient records in the provider's EHR system, thus reducing the time required to access those records at future appointments. If the provider has an EHR system capable of passing data back to the local RHIO server, then other providers will also be able to query that EHR system. Full interoperability of the FHIN will come about when all providers install EHR systems that can pass data records up to the local RHIO server for storage in the minimal data set.

7. Once the patient's visit is completed, the provider will delete the patient records from the 'active' list on the office computer. A record of the patient's visit should be recorded in the RHIO's minimal clinical dataset for use by other providers. If the provider has an EHR system the patient record can be uploaded automatically to the local RHIO as an element of the minimal clinical dataset for that patient.

In the FHIN model, the local RHIO server should store a minimal clinical dataset of patient records collected from providers registered with local RHIO, who have signed BAAs with the RHIO. This dataset will allow providers to retrieve information on patients almost immediately upon querying the local RHIO. This set of minimal data records will consist of only the most important details of the patient's health record, and will be returned first in all medical record queries. It is essential that the provider be able to record a patient visit and add data elements to the minimal clinical dataset at the RHIO server. This function should be enabled by the FHIN interface, or by the provider's EHR.

In any future clinical engagements with the provider, the steps outlined above will be much more streamlined because the patient's cumulative record will already be archived within that provider's account and will only need to be copied onto the provider's active list with any new medical records added. As envisioned, the health information exchange portal is primarily for

data access to external records. Other data input functions such as progress notes or other clinical documentation could still occur on paper or in an Electronic Health Record, if the provider has such a system. Certain data input, such as e-Prescribing, may be appropriate via the local exchange, but these issues should be determined at the local level.

The way in which the technical specifications of the FHIN server fit the clinical workflow could determine how well the FHIN is accepted by providers. As demonstrated, each step of the clinical workflow has a technical counterpart in the FHIN. The idea here was to link each of the steps in the workflow with its appropriate technical solution.

Minimal Clinical Dataset That Will Ensure Clinician User Adoption

The discussion above, that a health information exchange mechanism must 'fit' into the clinical workflow, highlights the need to be sensitive to the concerns of clinicians and their staff. Ultimately the success of any community heath data exchange hinges on end-user adoption. Critical to widespread adoption and use of the health information exchange via the FHIN will be the inclusion and sharing of clinical and administrative data that will entice the providers to use the exchange. User acceptability can also be achieved with a user-friendly portal that allows each provider the ability to customize to his or her workflow.

In speaking to providers, the following data were considered critical to enlisting them to use the health information exchange:

- Patient Demographic and Administrative Information: Age, gender, and ethnicity are clinically pertinent information that often impact care decisions.
- Diagnoses/Problem List.
- Listing of Providers: This dataset can be obtained particularly from provider-generated claims records. For many providers, knowledge of other providers who are involved in a patient's care can provide valuable insight into the patient's illness and the level of care provided. Furthermore, awareness of other clinicians involvement can facilitate greater coordination/continuity of care.
- Allergies.
- List of Previous and Current Medications.
- Laboratory Results: For many providers, showing lab results electronically was the obvious 'win' of any exchange. For them, the capacity to show laboratory results would replace the burden of having to request and receive fax copies of results.
- Radiology Reports: Radiology images need not be available within the FHIN, but the final dictated reports would be of significant value in the continuum of care. Consideration should be given to providing a link to allow the physician to view digital radiological images. Providers are aware that viewing digital images on the average computer or laptop monitor is less than optimal, but many providers would still use the system to view images if it were available.

- List of Previous Procedures: Clinicians were very interested in seeing a listing of the name and description of procedures and their correlated dates.
- Provider-generated claims records.

Recommended List of Data Fields for the FHIN White Paper Minimal Clinical Dataset

A workgroup was set up on behalf of the GHIIAB to define a Minimal Clinical Dataset. While a key driver for defining this subset of records remains user adoption, it should be noted that standardization on a set of fields also enhances the aim of interoperability, as it ensures that a consistent data set can be exchanged between RHIOs. The following also need to be noted:

- The presence of a field in the subset does not automatically mean that all fields can be populated using existing HL7 fields from data sources, rather this is a target to aim for.
- While not all fields may be able to be populated, the recommendation is that the RHIOs still 'stub' unused fields in to help ensure data interoperability.

*Administrative Data Elements*

1. Social Security Number
2. Last Name
3. First Name
4. Middle Name
5. Date of Birth
6. Gender
7. Race
    a. Race
    b. Ethnicity
8. Home Address
9. City
10. Zip code
11. County of residence
12. State of residence
13. Primary phone number
14. Next of kin
    a. Last Name
    b. First Name
    c. Gender
    d. Address
    e. City
    f. Zip code
    g. County of residence

   h. State of residence
   i. Primary phone number
   j. Relationship to patient
15. Legal guardian
   a. Last Name
   b. First Name
   c. Gender
   d. Address
   e. City
   f. Zip code
   g. County of residence
   h. State of residence
   i. Primary phone number
   j. Relationship to patient
16. Age to be calculated at the time of the data query. Formula = (Date of Visit – Date of Birth). Age reported in days for children up to 18 months, and in years for everyone else.
17. Insurance – recommended
18. Advance Directives
19. Provider
   a. Last Name
   b. First Name
   c. Telephone Number
   d. Date of last encounter (with patient)
   e. Specialization
   f. Provider ID
20. Location – facility name
   a. Location - ID

*Clinical Data Elements*

1. Diagnosis:
   a. Admitting diagnosis
      i. Date of Admitting Diagnosis
   b. Discharge diagnosis
      i. Date of Discharge Diagnosis
2. Source of ICD-9
   a. Provider ID
3. Location of ICD-9
   a. Facility ID
4. Problem List

a. All ICD-9 codes associated with medical encounters, ordered by most recent date

5. Orders
   a. Prescription name, including: medications, herbal medications, oxygen, ventilators, specialty equipment, specialty, prescribed formulas, etc.
   b. Filled prescription
   c. Date prescription filled
6. Lab Reports – based on HL7 feeds
   a. HL7 OBR -- Observation Request
      i. 4 Universal Service ID
      ii. 7 Observation Date/Time
      iii. 14 Specimen Rcvd Date/Time
      iv. 16 Ordering Provider
      v. 22 Results Report/Status Change-Date - Recommended
      vi. 24 Diagnostic Service Sector Id
      vii. 32 Principle Result Interpreter
   b. HL7 OBX -- Observation/Result
      i. 3 Observation Identifier
      ii. 5 Observation Value
      iii. 6 Units
      iv. 7 Reference Range
      v. 8 Abnormal Flag
7. Allergies
   a. Name of Drug / Agent
   b. Reaction (open text field)
   c. Date of Reaction
   d. Severity or Kind of Reaction (using pick list)
      i. Mild
      ii. Moderate
      iii. Severe
      iv. Unknown
8. Immunization Status (recommended pulled from DOH SHOTS record)
   a. Pediatric immunization status (based on CDC schedule)
      i. Diphtheria, tetanus, and pertussis (DTaP) vaccine
      ii. Measles, mumps, and rubella (MMR) vaccine
      iii. Haemophilus influenzae type b (Hib) vaccine
      iv. Hepatitis B vaccine (Hep B)
      v. Polio vaccine
      vi. Chickenpox (Varicella) vaccine

vii. Pneumococcal (PCV7) vaccine
viii. Influenza vaccine
ix. Rotavirus
x. HPV
xi. Meningococcal
xii. Hepatitis A

b. Adult immunization status
i. Influenza (flu)
ii. Tetanus/pertussis
iii. Pneumococcal disease

9. Pediatric Vital Statistics – Collected Up to 18 months
a. Height
i. Value
ii. Unit of Measurement
iii. Date collected
b. Weight
i. Value
ii. Unit of Measurement
iii. Date collected
c. Head circumference
i. Value
ii. Unit of Measurement
iii. Date collected

10. Vital Statistics
a. Blood Pressure
i. Systole
ii. Diastole
iii. Date of Measurement
iv. Location of Measurement
b. Height
i. Value
ii. Unit of Measurement
iii. Date collected
c. Weight
i. Value
ii. Unit of Measurement
iii. Date collected

## III. The Role of the RHIO in the Florida Health Information Network

The RHIOs and other health information exchanges play an important role as community "umbrella" organizations that bring health care stakeholders together and as network intermediaries between the providers in the local community and the FHIN. The RHIOs take on the responsibility of bringing providers together for the purpose of sharing health care data and integrating their disparate computer systems into a health care data network that can pass medical records among all participants. Often the first data exchange is on a small level, but the volume of data increases as the network becomes a reliable resource for providers.

When a provider sends a data request to the FHIN for patient records, the RHIO first checks its MPI for patient data stored by any of its provider databases, and returns that information immediately to the physician; the RHIO next sends the query to the FHIN server, which sends data requests to other RHIOs or to the specialized databases accessible to the FHIN. In this way, the RHIOs also serve as medical data "aggregators" for the FHIN, providing access to its MPI to all patient records accessible from providers participating in the RHIO, and passing along patient records when requested by a provider who is searching for patient records on the FHIN. The dual roles of the RHIOs are highly valuable to the FHIN.

The idea of regional health information organizations (RHIOs) was first articulated by Dr. David Brailer, Director of the Office of the National Coordinator of Health Information Technology as a local corollary to the NHIN. He argued that RHIOs are critical to the success of health information exchange because they are the "business conveners" who bring together stakeholders in the local health care community.[7] The function of the RHIO is to work in the local community as a governing body, developing common policies, common security and privacy infrastructures and a sustainable business model for health information exchange, as shown in Figure 1. In Dr. Brailer's view, the RHIOs would collaborate with the NHIN to bring about a nationwide infrastructure of interoperable networks.

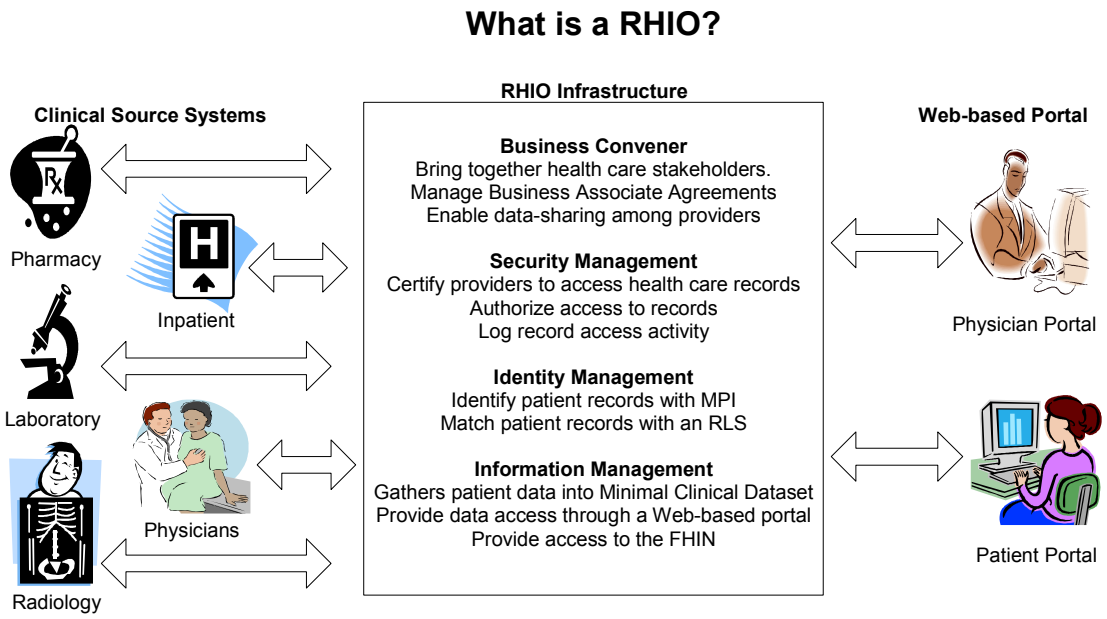
At the Healthcare Information and Management Systems Society (HIMMS) 2006 conference in San Diego, Dr. Brailer proposed that statewide RHIOs could work as portals to the NHIN for health information exchange within the state.[8] This statement is quite appropriate for the FHIN, which proposes to link together local RHIOs around Florida into one health information network. Each RHIO in the state can leverage health care data from participating providers, but each is limited by geographical constraints. The full value of the FHIN will come from transporting medical records among the RHIOs, and providing a connection to medical data in other states – an important function given all of the visitors to Florida. The benefits coming from the local RHIOs bringing together health care stakeholders, and initiating data-sharing among diverse providers are amplified when the FHIN connects the different RHIOs together.

Numerous RHIOs have developed in the United States in the past five years, generally forming to solve local problems of information-sharing among physicians by using available computer

[7] Tommy G. Thompson and David J. Brailer, MD, PhD, *The Decade of Health Information Technology: Delivering Consumer-centric and Information-rich Health Care*, July 21, 2004.
[8] Brewin, Bob (Feb. 13, 2006). *Brailer: State RHIOs crucial to health IT*. Government Health IT. Retrieved from http://www.govhealthit.com/article92325-02-13-06-Web on February 22, 2006.

networks. Each RHIO is unique in its genesis, arising out of local needs and initiative. A few can be cited as examples. The Indiana Health Information Exchange (IHIE) developed out of a core of clinicians at the Regenstrief Institute and has spread its network to include providers in greater Indianapolis and the surrounding region. The Utah Health Information Network (UHIN) grew out of a coalition of payors, providers and the state government. The UHIN's intent was to create value for all participants and is comprised of providers, who pay an annual membership fee and payors, who pay a per transaction fee.

Figure 1. Schematic of RHIO Activities?




The Tennessee Regional Demonstration Project developed from an initiative in the Vanderbilt University Medical School, with funding from the Agency for Healthcare Research and Quality (AHRQ), to build a health information exchange in Memphis and surrounding areas. Finally, the California Regional Health Information Organization (CalRHIO) was formed as an overarching health information network that is attempting to interconnect several smaller health information projects already established in California. In every case, the development of the health information organization is paralleled by the creation of a computer network for sharing medical records. Several organizations track RHIO development, and are a good source of information about them. These organizations include eHealth Initiative (http://www.ehealthinitiative.org), the Markle Foundation, Connecting for Health Initiative (http://www.connectingforhealth.org) and HIMSS (http://www.himss.org/asp/topics_rhio.asp).

In Florida, the development of RHIOs has accelerated in the past year. In 2005, three not-for-profit corporations organized as RHIOs in the state, all of them responding to a core of providers. In Tallahassee, the Big Bend RHIO formed at the initiative of physicians, hospitals and a vendor to provide medical records, radiology imaging and lab results online. The backbone of this RHIO is the pMAN optical fiber network installed by ElecroNet Intermedia Consulting for the radiology community. In Tampa, the Tampa Bay RHIO was formed through a collaboration of the Tampa Bay Partnership, faculty at the University of South Florida, and Gold Standard, a company specializing in the pharmacy prescription data. Gold Standard recently worked with the

Department of Health and Human Services, Medicaid and private vendors to recreate prescription records for several million refugees from Hurricane Katrina. The Tampa Bay RHIO will begin providing prescription and laboratory records to physicians via PDAs and over the Internet, using a system developed by The Northwest Florida RHIO began as a collaboration among physicians, hospitals and a vendor. Other health care associations in the state are moving toward health information exchange and are bringing together providers to begin sharing medical data. Each of these RHIOs, and others, will be connected and have access to patient records held by providers in the RHIOs, via the overarching FHIN infrastructure.

One issue of critical importance for RHIOs is the location, accessibility and ownership of medical records. Most providers maintain their own patient records and are often hesitant to release them outside of their domain. A data-sharing orientation must be fostered by each RHIO. But even when a provider does become willing to exchange records, the question of where the data should reside still must be answered. There are two, polar models that cover most of the data-sharing arrangements: centralized versus decentralized or federated models of data location.

In a centralized architecture, all of the data reside in one locale, generally a central server. The advantage of centralized data is that security, authentication and system management are centralized; a single set of operational and technical requirements for the system are specified and the data are available around the clock.[9] Another benefit of the centralized system is that all data could be backed up in a separate location. One drawback of centralization is that data are duplicated and the total volume of data in the database could become overwhelming. In a decentralized or federated model, the data reside in the provider system and are accessed directly from the provider's database. Data can be accessed in a couple of ways. Using a peer-to-peer network among providers, each provider would contact the RHIO server to locate the appropriate records, then retrieve those records from the corresponding location. A second approach would rely on the RHIO server to act as a trusted agent for all information exchange, and when requested by a provider would locate, pull and distribute the data from the appropriate provider databases. These issues, among others, are discussed in greater length in a later section.

Each of the RHIOs in Florida holds a vital position in the development of the Florida Health Information Network. While the FHIN will provide statewide connectivity, the RHIOs are responsible for working at the local level with providers, laboratories, radiology labs, clinics and administrators at all levels. The RHIOs shoulder the burden of convincing providers to share their patient records and of getting Business Associate Agreements signed. The RHIOs take on the task of building technical capacity in the health information exchange and of enabling providers to pass records among their different systems. The RHIOs work with physicians to provide them patient data on demand and to offer training and education in electronic data transfers. Finally, the RHIOs work with the FHIN to create a seamless health care information network across the state that is accessible to every provider and benefits all of Florida's citizens.

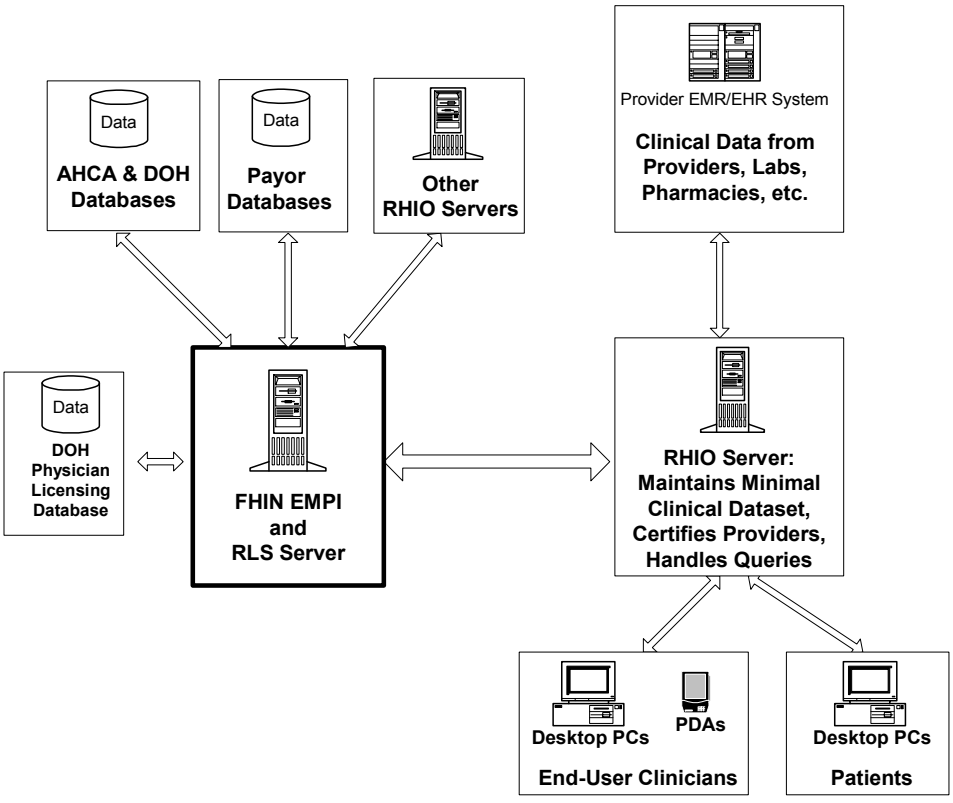
[9] US Department of Health and Human Services. *Summary of Nationwide Health Information Network (NHIN) Request for Information (RFI) Responses, June 2005*. Retrieved from

## IV. Building the Florida Health Information Network

The FHIN is envisioned as a statewide health information infrastructure that will enable health care professionals to access a patient's medical records from any provider database connected to the network over a secure Internet connection. The FHIN represents a collaborative effort between the public and private sectors, state and local governments, RHIOs and health information exchanges, providers, employers, consumers, health plans and payors. The FHIN proposes to interconnect health care providers across Florida to facilitate the sharing of health care data without regard to where in the state the consumer resides or where the health care was delivered. The FHIN infrastructure will allow local RHIOs the greatest amount of flexibility in implementing their plans to integrate health care data in their communities.

The FHIN infrastructure will be built around a central server that will maintain connectivity among RHIOs or other health information networks in the state. The FHIN server will hold an EMPI, an RLS, and the software to query database servers maintained by the RHIOs, by other state agencies, in provider-generated claims databases and the NHIN, when it is built. The FHIN architecture is specifically designed to give the RHIOs the greatest amount of flexibility to accommodate the needs of their constituent health care providers. The FHIN will make use of the existing connectivity and data storage capability of health care systems whenever possible. Many of the hospitals, clinics, primary care facilities, pharmacies and labs in the participating RHIOs have invested in in-house computer systems that will form the basis for the secure, timely and accurate transmission of their health care information.

Figure 2. Model of the Florida Health Information Network



The FHIN will use existing connectivity standards whenever possible. The interface between the statewide server and the regional servers will be based on web services standards and common internet protocols and XML/HL7 standards for optimum interoperability. Such a standardized interface will enhance the portability and scalability of the FHIN, and of the RHIOs around the state. The ease of transmitting XML schema to participating organizations facilitates the future growth of the FHIN. Figure 2 displays a conceptual diagram of the FHIN server and its interconnection to RHIOs, state agency and provider-generated claims databases and the Department of Health physician licensing database. Each RHIO or database can be treated as an independent local network, interconnected to all other regional networks through the central FHIN server.

The FHIN EMPI will consist of a registry of patient identifiers for every patient in Florida who has a medical record held in one of the databases connected to the FHIN. This EMPI will complemented by RLS, which will find records of patients identified by the EMPI. When a patient record request comes to the FHIN, its server will use the FHIN RLS to connect to the specific servers in a RHIO, or other database, with the RHIO being responsible for matching the patient record. When matching patient identifiers are found, the RHIO will locate and retrieve the patient's health care records and return them to the FHIN, which will in turn and make them available to the requesting provider. Another function of the FHIN server will be to connect to the Department of Health physician licensing database to check the license status of physicians and other health care professionals who want to access medical records using the FHIN. The ability to use the Department of Health physician's licensing information to authenticate providers will be a strong asset in maintaining network security.

It is the recommendation of the FHIN Network Security Workgroup that each RHIO make a credentialing authentication call when a clinician logs into the local RHIO for the first time to ensure that the clinician (or person authorized by the clinician) is credentialed in the State of Florida.

The FHIN Network Security Workgroup also recommended that the credentialing database be used to verify clinicians at the point they are registered as authenticated users in a RHIO.

The FHIN server could also connect to Florida state agency health care databases, and to provider-generated claims databases that cover claims records for Florida patients. For example, the Department of Health child immunization program, the SHOTS, maintains a statewide, centralized electronic immunization registry that keeps track of immunization records of all children in Florida. The FHIN could access the SHOTS database, either as a portal to deliver providers to the website, or as part of a database query which returns immunization data on a pediatric patient. Another health care database that could be accessed by the FHIN are the inpatient and outpatient records held by the State Center for Health Statistics in the Agency for Health Care Administration. These records contain ten years of historical health care information on every patient who has received care in a Florida hospital or in an ambulatory surgical facility.

By making these records available to providers, the FHIN could offer physicians background information on patients that covers diagnoses, procedures, operations and frequency of hospitalizations, among other information. Other health care databases are held by the Division of Medicaid in the Agency for Health Care Administration, the Department of Education, the Department of Elder Affairs, the Department of Veteran's Affairs, The Department of

Corrections, the Department of Juvenile Justice, the Agency for Persons with Disabilities and the Division of Workers' Compensation in the Department of Financial Services.

Another source of health care data open to the FHIN is from provider-generated claims records. Such databases carry information on prescription drug history, lab history, radiology history, history of visits to doctors and hospitals, immunization history and diagnosis details. Because the claims data are continually updated, there is no time lag as exists with the inpatient date reported to the State Center from hospitals. Physicians can check on the medical history of a patient and receive up-to-date information. The following case study looks at a provider-generated claims system, Availity, that is a potential partner to the FHIN. Availity is jointly owned by Humana and Blue Cross Blue Shield of Florida, and is developing a web-based portal for delivering health care information to physicians. Availity offers a service that is secure, HIPAA compliant, audited and accessible only to authorized providers. The health record system could be made available through the FHIN, and could offer enhanced access to provider-generated claims records of other major companies such at United, Aetna and Cigna. The following case study is intended as an example of a functioning health record service, similar in architecture to the FHIN, and as an example of a health record database that can be accessed by the FHIN in response to a providers request for patient records.

It needs to be noted that some physicians in the FHIN Minimal Clinical Dataset Workgroup expressed strong opinions about the relative value of claims data versus data from EMR and other source clinical systems, indicating they felt there was value in claims data as supplemental data, but not as a replacement for primary data.

The Availity Provider-Generated Electronic Claims Record

This case study is an overview of an Internet-based healthcare application with significant adoption throughout the State of Florida. By providing Internet access through open standards technology and maximizing stakeholder connectivity, the application has successfully interconnected thousands of providers to hundreds of payors who represent millions of lives in the State of Florida.

*Background*

Availity was established in 2001 by two large competitive payors (Blue Cross Blue Shield of Florida and Humana) to address HIPAA, non-electronic business (paper, phone, etc), and the growing proliferation of provider portals and proprietary administrative systems in Florida. The system was designed to provide real-time standards-based connectivity between providers and any payor who wished to join the network. By establishing secure, real-time Provider access through a single portal to a high-percentage of Florida payors (e.g. Aetna, Blue Cross Blue Shield of Florida, Cigna, Florida Hospital Healthcare System, Humana, Vista Healthplan), adoption of the Availity system grew to over 13,500 registered Provider sites, representing over 90% of total providers in the State of Florida by 2005.

*Architecture and Accessibility*

The Availity architecture was designed and developed using open standards and industry proven technologies. Utilizing the Internet and associated browser technologies made the technology relatively accessible to providers throughout the state. As the use of broadband Internet access

increased, so did the adoption and use of the system. All communication and functionality was designed to be secure through the use of authentication, authorization, encryption and certificates.

To further the reach of the real-time functionality beyond the portal, the company published business-to-business (B2B) X12/XML specifications to allow the seamless integration of provider management and hospital information systems. Standard batch EDI guidelines were also published because of the majority of technology vendors not having real-time capabilities; over four hundred providers opted to use the batch integration option. However a handful of vendors initially used the real-time B2B option and that number has steadily increased (from seven in 2003 to about twenty in 2005). The B2B connection requires that vendors authenticate and authorize their respective end-users, while the vendor-to-Availity connection is through a secure and authenticated connection.

*System*

The real-time system/portal was developed for submitters of information (e.g. providers, billing services, vendors) to securely transmit administrative transactions in HIPAA-compliant X12 format to the Availity gateway. Once received, the system parses the transaction to ensure regulatory compliance and also to route the transaction to the appropriate payor in the appropriate format. Once the payor receives the transaction, the payor processes it and returns a response, which is then returned to the submitter only if it passes compliance edits.

This model is a federated model which does not require centralized storage of patient data. When information is requested in the proper format with the appropriate identifying keys (Payor ID, Patient ID, Patient Name, DOB, etc), the system routes the transaction directly to the source system. By explicitly identifying the payor, the patient information is then handed off to the appropriate payor for proper identification in a delegated MPI model.

The federated-data, delegated-MPI model will be the initial foundation for a multi-payor-based health record (PBHR). Using the existing infrastructure and data that are already being sent to and stored with the payors, requests for a PBHR will be routed through the system to the respective payor. Once this model has been piloted in the field, an MPI will be introduced into the system at Availity.

This MPI will keep the minimal amount of data to accurately identify individuals and locate associated relevant data sources, initially payors. To access relevant payor data, an individual's active or previous identification number with a payor can be used. Participating payors will need to use a standard electronic transaction such as the ASC X12 834, Benefit Enrollment and Maintenance transaction, to update and maintain the MPI.

In future phases, additional data sources will participate in much the same manner. The expanded use of the X12 834 to capture and transmit additional demographic information has been discussed by entities such as the National Committee on Vital and Health Statistics (NCVHS) and the Centers for Medicare and Medicaid Services (CMS). Whatever standard is eventually adopted for additional data sources must be supported by the commercial payors as well as the government for interoperability support.

Using the standard connectivity and security outlined in this case study, along with state operating guidelines and business-rules, Availity and other health information networks could connect to the FHIN for appropriate uses such as the coordination of care, access to RHIOs, and access to government data. Access to Availity claims records via the FHIN would offer a tremendous boost for the delivery of electronic health care information, and could lead the way for other RHIOs and health care information exchanges to share their records across the FHIN.

## V. Technical and Non-Technical Issues Facing the Florida Health Information Network

RHIO Architecture on a Sliding Scale

Having discussed conceptually the architectures of the decentralized or federated and the centralized models for RHIO architecture currently being debated in America, it needs to be noted that there are a number of variations that exist between these two extremes. In his article entitled "Federated and Centralized IT Architecture Models for Portable EHRs,"[10] John Quinn discusses various RHIO architectures and attempts to define architectures in five or six distinct models. While that is a valid and useful method of classification, there are nonetheless many more variations between centralized and decentralized that could be proposed for RHIO architectures.

At the core of these discussions lie three or four key architectural decisions, which in turn are influenced by technical, policy, political, cultural and financial factors. In this section we will define a sliding model which can be used to understand the differences between the centralized and decentralized structures, which will in turn be used to build the framework for a mixed-mode architecture. There are four models of server architecture that can be identified:

- Fully decentralized
- Decentralized with the edge servers at the source location
- Decentralized with host servers at the central location
- Fully centralized

It should be noted that in each of these four models along a sliding scale from centralized to decentralized (and any other potential variations that may arise) there is a duplication of data in the central repository and in the edge and host servers. In addition to this, if providers of data will not permit direct access to their clinical systems, even a decentralized model will end up with a duplication of data, as the providers will have the expense of providing edge servers. In the final analysis, one of the primary drivers behind the adoption of decentralized systems ceases to be a factor. Case studies of operating decentralized systems may reveal if such systems are indeed less expensive than alternative solutions.

*Benefits and Challenges of Decentralized and Centralized Servers*

Conceptually, the appeal of a decentralized RHIO architecture is clear. The footprint of the hardware required to run the RHIO is much smaller, resulting in lower central costs, lower replacement costs and lower operating expenses. Decentralization avoids a central architecture that requires set up and maintenance, and which keeps growing in size into a larger centralized database. As is quite rightly pointed out, the storage of data in a central database and in its original source location results in a duplication of clinical data. In addition, the appeal of being able to retrieve data from a source location is extremely appealing, when compared with storing the data in a central location with the potential implications of compromise of data security. For

[10]John Quinn, *Federated and Centralized IT Architecture Models for Portable EHRs, HCT Project Volume 3* (11/14/2005). Retrieved from http://www.hctproject.com/documents.asp?d_id=3545# on January 9, 2006.

many, the benefit of the decentralized model lies partially in political concerns that the RHIOs and the NHIN will be viewed by the general public as leading to "big brother" databases.

Adherents of the central server model will point to what they consider practical flaws in a decentralized model. In particular there is a concern over network latency, and the ability to collect information from a number of sources in real time to allow for useful clinical data to be displayed in a timely manner. Network latency refers to the time delay between requesting information and having the data returned, and is often related to the volume of network traffic. In addition, it has often been pointed out that availability is a sum of all of the subsystems required to build a complete record in a decentralized model, and that all source systems will be online 24/7. While this may be a valid assumption in the case of most larger health care providers and state agencies, many question the ability of smaller providers and primary health care physicians to provide systems which would be online at all times. Even in a decentralized model, the centralization of a minimal information set makes sense to provide a "back-up" of service when a system is not expected to be up 24/7, such is in a single physician practice that shuts off its EMR at the end of the day. This issue is especially acute during large-scale disasters, at the time when access is needed most of all.

The analogy which is sometimes employed mirrors the experience of those who used Napster in its heyday. One may recall the Napster logo being presented on the screen as the basis for the Santa Barbara decentralized architecture at the July, 2004 NHII annual summit. While the appeal of a decentralized model is its ability to locate multiple sources of information quickly, as with peer to peer music-sharing software, anyone who used Napster on a regular basis became all too aware that it could take up to two minutes to fully locate all songs. In addition, the retrieval time of the individual songs varied enormously depending on the type of network connection, the amount of traffic that the source system was experiencing, and the technical capabilities of the source system.

It may be validly pointed out that the source systems in peer to peer music-sharing software typically involve PCs, and not network servers. Nonetheless the widespread use of peer to peer systems for the accumulation of clinical data from a variety of source systems, including providers, payors, the state servers, large physician practices and small physician practices remains unproven. The partitioning of domains relative to the proposed traffic must always be taken into consideration; in this context the ability to establish RHIOs that service the appropriate geography should be considered. The FHIN needs to have proactive market strategy to target the RHIOs geographically in a way that will result in the highest level of adoption in the shortest amount of time. A Service Level Agreement should be in place that ensures a certain level of performance within a local geography, with lower service levels as the distance increases from the "home" RHIO.

A second aspect of the decentralized model that needs to be more carefully examined is the often quoted contention that the decentralized model is less expensive than central storage. The primary logic behind this argument is that sending data to a central storage location and storing data at that location requires a much larger information technology footprint, and hence is more costly due to the associated operational and regular replacement costs associated with the centralization of data.

This argument may have been valid if, as was originally postulated, providers allowed access directly to the source systems. It is built on the premise that the original holders of the data only have a minimum expense associated with the rollout of a decentralized system. The reality is that any large to medium size provider is unlikely to allow a decentralized RHIO direct access to the clinical systems. Providers spend a great amount of effort ensuring that clinical systems are sized correctly, i.e. not too large and not too small. Allowing these systems to be opened up to queries and access from outside entities, particularly with the potential long-term aim of allowing queries of large sets of data for research purposes, would make it impossible for enterprises to do accurate capacity planning. In addition, to allow outside entities direct access to clinical systems, holes would have to be opened in firewalls, allowing an unprecedented access level to networks within the provider systems. Finally it needs to be noted that should a system become compromised through the access from a RHIO, the provider, under HIPAA, could be responsible for any breach. The Security Rule portion of HIPAA requires that the owner of the protected health data needs to take "adequate" security measures to protect the data. Thus, providers would be opening themselves to new levels of responsibility.

Most large providers have expressed the opinion that in order to meet the requirements of decentralized RHIOs, they would be required to publish the internal data to a staging area, called an edge (or proxy) server. This infrastructure would have high availability, would be required to reside in a Demilitarized Zone (DMZ), and would certainly require expenditures that the providers would not otherwise be incurring. Even then, the network is not totally safe, but may be more susceptible to outside attacks due to the heavily used data pipeline connection that may make it a more attractive target by potential hackers. Hackers often look at where the most data are flowing as a target for their attacks. The fact that the data flow through an edge (or proxy) server in the DMZ, however, minimizes the potential for compromise since the hackers would most likely not be able to access the area on the network where the primary data reside. The decentralized model using edge servers could provide the best balance of security and decreased latency, although it would increase cost over a purely decentralized model.

An alternative to having edge servers located at each individual provider, is the concept of having individual servers located at the central location, thus allowing the data from each entity to be physically and separately stored. This is similar to the Indianapolis model in which data are stored in separate data vaults. In addition to logically separating the data, there is also a physical separation of servers. Once again this results in a duplication of data, and increased operating expenses, and increased ability for error, and involves a much larger central footprint.

*Mixed-mode Model*

After considering the relative advantages and disadvantages of both centralized and decentralized models, an argument can be made for the adoption of a mixed-mode model. A version of this model was adopted by the National Health Service (NHS) in the UK. At the core of the mixed-mode model is an unlimited central data repository containing the core clinical information most frequently identified by clinicians as being the data they would wish to have displayed in a structured data interface for ease of use.

One of the concerns of the decentralized model is that while data may be gathered from a variety of sources, in order to display that information in a longitudinal health record, the data need to be merged, and data elements need to be matched, vocabulary and coding need to be matched, and

the data need to be provided in a structured format. Too much data can present as much problem as too little data, and if an interface were required to delve into each patient and interaction record in order to gain a complete view of the patient's health, then adoption would be a problem. A simple example of this would be combining the blood pressure, weight and pulse taken during most medical examinations. The true value of a complete patient health record lies in its ability to take these readings and present them in a single chart, regardless of who took the readings, or where they were taken. Ultimately this may include readings taken by the patient at home and entered into a personal health record.

There are two major standards currently proposed for reporting patient records. A standard called the continuity of care record or CCR has been taken up by the standards body, ASTM, International. The standard was recently approved by the members of the ASTM, and is in the process of being published. HL7 and ASTM have agreed to work together to harmonize the CCR with the HL7 clinical data architecture standard. The CCR is a collection of clinical elements originally intended to be obtained at the end of a clinical visit and transmitted electronically to the next health care provider to allow for automatic entry of data into electronic medical records systems. This would operate to provide the most pertinent data within a time frame required to provide high quality health care, and to help eliminate the clipboard so frequently experienced by patients in the United States who are treated concurrently by more than one provider. Data elements would include but are not limited to demographic data, insurance information, allergies, lab tests, medication history, and any other recent medical history.

The second major standard is the clinical data architecture or CDA, which is part of the Health Level 7 (HL7) family of standards. The CDA defines the extensible markup language (XML) required to exchange clinical messages by specifying the structure and semantics of clinical documents. A CDA document can include text as well as multimedia content such as images and audio recordings. The CDA document is designed to be sent inside of an HL7 message, but it can also exist independently of the HL7 message. Several guiding principles have driven the design of the CDA. These include giving priority to documents generated by clinicians involved in direct patient care; minimizing the technical barriers needed to implement the CDA; promoting longevity of all information encoded according to the CDA; and promoting exchange independent of the underlying transfer or storage mechanism.[11]

Both ASTM and HL7 are discussing the harmonization of the CCR and CDA into one standard. The CDA has a Care Record Summary (CRS) that contains CCR content, but delivers it using the CDA structure. This allows vendors a common pipe to support both medical summary information exchange as well as upcoming HIPAA Clinical Claims attachments, which will also use CDA. The current CCR standard defines its own structure, which would require vendors to implement two schemes to essentially carry the same information. Numerous organizations support the harmonization of both standards into one standard; these include: the Department of Defense, the Veterans Affairs Administration, the American College of Physicians (ACP), the Radiological Society of North America (RSNA), the American College of Cardiology (ACC),

[11] Dolin, R., et. al. (2001). *The HL7 Clinical Document Architecture.* J Am Med Inform Assoc. 2001 Nov–Dec; 8(6): 552–569. Retrieved from http://www.pubmedcentral.gov/articlerender.fcgi?artid=130066, on March 3, 2006.

the Healthcare Information and Management Systems Society (HIMSS), the Electronic Health Record Vendors Association (EHRVA) and Integrating the Healthcare Enterprise (IHE).

The mixed-mode architecture would call for a subset of clinical records defined in the harmonized CCR/CDA standard. At the end of each clinical encounter the provider would supplement and update the relevant fields of the harmonized CCR/CDA standard based on the latest encounter, and that data would be used to update the central harmonized CCR/CDA. For electronic medical record systems to be able to make use of the harmonized CCR/CDA, the data could be imported directly into the system, eliminating the use of patients' clipboards. For those systems unable to import data in harmonized CCR/CDA format, clinicians would be able to go into the clinical portal, call up a patient's summary health record, and use that to enter any pertinent information that is not currently in their own electronic medical record. For the clinician there are multiple benefits to the adoption of the mixed-mode system. These include rapid response times, with the most pertinent information being displayed in a structured and organized manner, elimination of the patient clipboard and resultant errors, and the potential for automated entry of data through the use of the harmonized CCR/CDA.

It should be noted that there are technical challenges associated with adopting a mixed-mode model. In the first instance it assumes that providers will be able to provide HL7 formatted messages that can consistently be identified and associated with the given patient and used to update the central record. Secondly, it does not eliminate the need for clinicians to be able to drill down into individual patient records in the delivery of care. In order to resolve that problem, decisions will need to be made regarding which data elements should be stored and where they should be stored. It needs to be noted that the central storage or storage on edge servers of CAT scans and MRI images can take up vast amounts of storage, and due to their size can pose significant challenges to bandwidth and response time.

While the storage of CAT scans and MRI images would decrease bandwidth to a certain degree, the actual impact may not be as significant if the edge server is located in the DMZ, e.g., it would not adversely affect the bandwidth of the provider's intranet. It is difficult to justify duplication of large Picture Archiving Communications System (PACS) archives of images. As clinical content becomes richer (and larger), the need to centralize duplicate information will grow, resulting in more information being pushed to the edge servers, hence there is a case for mixed-mode architecture which will involve edge servers. Nonetheless it is recommended that the State of Florida seriously consider the adoption of the harmonized CCR/CDA standard, or a subset as the basis for partially centralized storage in a mixed-mode model.

*Minimal Clinical Dataset*

In considering the issue of network latency, a three-stage model of data access is proposed for the RHIOs and the FHIN. In this model, when a provider searches for a patient's records, a priority set of data stored on the RHIO server will be returned to the provider at once. The data query will then search through records held by RHIO while it sends the query on to the FHIN to search for records in other databases and RHIOs. At the first, synchronous stage, the data can be returned with little time delay because it is stored in a clinical dataset on the RHIO server. The other two asynchronous stages can take longer to return patient records to complete the patient's record history. Whether the RHIO is based on a decentralized, centralized or mixed-mode model, the authors recommend that the RHIO store a minimal clinical dataset on the RHIO server.

The minimal clinical dataset will be made up of data that are indispensable for the first assessment of the patient's records. It might hold the most recent lab values, or prescription information. The key concern is that the dataset will return priority information on a patient's health status to the physician, with little time delay. The data should be selected and stored based on the harmonized CCR/CDA standard, and all providers, or the RHIO, should be able to update these data fields as they change.

In January 2006, the Governor's Health Information Infrastructure Advisory Board recommended that the Agency for Health Care Administration form a workgroup to address the development of the minimal clinical dataset, the data fields that need to make up the minimal dataset, and how to implement the harmonized CCR/CDA standard to access data that conforms to only one or the other standard. Recommendations from this workgroup have been included in this draft of the paper.

Authorization and Authentication of End Users

In dealing with the need to authorize and authenticate users to access the FHIN, several issues will need to be resolved around the trust relationship between RHIOs, and between RHIOs and the FHIN server. At issue is the question of which entity handles the authentication and authorization of end user requests when the request is passed from the RHIO to the FHIN server and on to another RHIO. A number of options are available, as will be discussed in this section.

Two key concepts need to be defined in order to adequately cover the discussion in this area: trust and latency. These terms are being used in a looser technical sense than may be strictly applied by security or IT professionals, but conceptually their use and application remains the same.

*Trust Relationships*

In the context of this white paper, the trust relationship between servers exists when one server requests information from another, and the requested server does not need to authenticate the individual user request because a trust relationship exists between the two servers. This response is premised on the reasonable assumption that the requesting server itself authenticates all user requests prior to forwarding them to the requested server. The trust relationship thus implies a certification process. At issue is the question of whether both the FHIN server and RHIO authorization and authentication mechanisms need to be able to individually identify requests from remote locations.

A number of servers house clinical information on behalf of the state, access to which is governed by statute or state regulation. In many cases it is stipulated that data cannot be provided without the positive identification and authentication of the requesting party. At a practical level this means that a user logging onto a local RHIO cannot expect the local server to make a request for data to one of the states entities using a pure trust relationship. The requesting server would need to pass the user credentials on to the state system, prior to the state system being able to pass the information back to the RHIO.

At a practical level, retrieving state-held data may require access to state agency servers to done directly, with a connection from the end user's PC. Alternative mechanisms will need to be investigated, including the RHIOs making the request on behalf of the user, and passing the

information back to the user via the RHIO network, or the FHIN providing a direct portal to the state agency website. The type of trust relationship defined above between either the RHIO or the FHIN server and one of the governmental entities may not be permissible under current guidelines, and changes to existing legislation may be required to allow this.

The FHIN Network Security Workgroup endorsed the concept of trust relationships between the RHIOs and the FHIN server.

Also at the core of the discussion is the relationship between both the end user and the RHIO, and the provider entities and the RHIO (provider entities in this context referring to providers of data to the RHIO). In almost all of the existing RHIO models, the HIPAA business associates agreement (45 CFR §160.103, 164.502(e)(1) and 164.504(e)(1)) is an acceptable mechanism for sharing of data with the RHIO, based on the assumption that the collocation services provided by the RHIO are business functions that could not be performed by the individual entity itself.

In most models the agreement calls for a business associate agreement, or BAA, to be signed between the entities and the RHIO, but not between each of the entities themselves. In other words, there is the recognition that if the RHIO governance models required every entity to have a business associate agreement with every other entity, as the number of entities becoming members of the RHIO increases, the manageability of the legal agreement becomes increasingly costly and administratively burdensome. Having a business associate agreement with only the RHIO means that individual entities would not be required to have a business associate agreement with other participating entities at a local level, nor with the FHIN because the data being shared are for the benefit of the patient. There is an exclusion within HIPAA the when sharing of electronic patient health information (ePHI) is for "treatment, payment or operations," and sharing of this data would be in the interest of treatment of the patients who have agreed to participate in the program. The same general standard applies when a local physician refers a patient to another local physician and physically delivers the medical record to the referred physician.

If clinician A connects to RHIO A in a given geographic area, RHIO A will be expected to know who the clinician is, as well as what rights he or she has to access patient data within that RHIO. If this type of authentication model were to be extended to all RHIOs and to the FHIN server, we would end up with a situation in which every single RHIO would have to be aware of every single clinician within the state, even though in many circumstances a clinician may never request information from a given RHIO (for example a clinician in North Florida requesting information from the Miami RHIO).

In order to deal with a business associate agreement between the provider and RHIO only, a trust relationship would need to be set up between RHIOs. One trust model would assume that any clinician who has access to data from one RHIO, would automatically have access to patient data for any patient for whom they have been previously authenticated and authorized by any other RHIO. Under these circumstances a service account is used between RHIOs which contains information about the requesting clinician, but does not directly authenticate the condition. This could be referred to as a semi trusted connection – the trust relationship exists between the RHIOs, but information regarding the request is still to be stored in a database for auditing and logging purposes. An alternative trust model would be that information is requested from one RHIO by another RHIO, and the logging information which is stored relates only to the RHIO

requesting the information. Under these circumstances the requesting RHIO is completely trusted by the data provider, the second RHIO, and it becomes the responsibility of the requesting RHIO to do logging and auditing of requests.

The ideal scenario would probably involve using both mechanisms, i.e. both the requesting RHIO and the requested RHIO would keep detailed log information about remote requests. It would be in the interest of the FHIN to maintain an audit trail of all data requests among RHIOs, in addition to the logging made by the RHIOs themselves. However, in both models, there is an explicit understanding that the requesting RHIO does not need to explicitly authenticate and authorize the requesting clinician because the RHIO providing the data, or the FHIN, has already authenticated the user. Within the model being proposed in Florida, the FHIN would play a crucial role in this process, ensuring that all data shared meet with HIPAA requirements and state statutes.

*Network Latency*

A brief discussion is required to understand the effect of network latency on end user performance. Transmission Control Protocol/Internet Protocol (TCP/IP) is the protocol used by Internet and intranet applications. Information is transmitted from one system to another using a stream of data. In order to manage the data effectively, it is broken down into a number of packets or pieces of information. Each packet is sent and a response is requested to ensure that the information was correctly received before the next packet of information is sent to the destination machine. This is called a synchronous request, as opposed to an asynchronous request where information is sent and a response is not waited for. Synchronous and asynchronous requests can occur either at a micro level (such as the communication process when packets are sent), or at a macro level. The implications of synchronous and asynchronous requests at a macro level will be discussed elsewhere in this paper.

For the purpose of the discussion around authorization, authentication and response time, suffice it to say that latency, or the amount of time spent traversing a network, increases with geographic distance. Latency is measured in milliseconds, or thousandths of a second. While it may be difficult to imagine that any time slice measured in periods as small as that may have an impact on performance, one needs to remember that any given piece of information may be broken down into a number of packets. If, for example, an average network latency across the Internet is 100ms, if a piece of information were broken down into ten packets that would translate into one second of wait time for the end user.

The overall result of latency is an increase in the end user wait time; this depends on the volume of information being sent out and requested, and the geographic distances being traversed with their associated latency times. Even at a local level, latency can present challenges in a completely decentralized RHIO model. For example, image files can be extremely large – in particular CT scans and magnetic resonance imaging (MRI) objects.

To help understand the implications of latency, let us consider the use case of a clinician connecting to a local RHIO and requesting patient information. If, as is commonly proposed, the Internet is used as the mechanism for retrieving information from a RHIO, latency time across the public Internet is variable and can be affected by a number of factors, including virus outbreaks, new releases of software being downloaded across the Internet by multiple users, and streaming media.

The end user connects to a RHIO, which challenges the user for his or her credentials. Once those credentials are accepted and authenticated, the user is faced with the screen where he or she can type in criteria to select a patient's records to view. In the event that the MPI or record locator service being used does not permanently pre-match patient records, the matching of patient records would need to occur before the query could proceed. This may be followed by the end-user manually choosing which records to match. In a distributed model, once data are requested, the request is sent to each of the participating entities.

The latency issues associated with this model are discussed elsewhere within this paper, however end user performance will be directly affected by the nature of the network connection between the RHIO and each of the participating entities, as well as the individual response time and scalability of each system providing data. Simply put, there is a significant difference between being able to display on screen a list of records from a local database, and the ability of the RHIO to retrieve each of those records dynamically, on the fly, across a wide area network, or across the Internet. In each case the latency of end user wait time for each of these steps can be measured in seconds or parts of the second. The net effect, however, may mean longer and unacceptable wait times for the clinician. One of the requirements we have heard repeatedly from clinicians is rapid response time. The adoption of any IT system can be severely hampered by inadequate response times or lack of user satisfaction.

*Network Security and Community Confidence*

At both the state and community level it is imperative that network security be an integral part of the FHIN and RHIO infrastructure development. Security must not be an afterthought. Critical to FHIN activities is building community trust and confidence that the protected health information (PHI) of patients will, in fact, be guarded. As the FHIN sets the cornerstone for an interoperable world of sharing PHI via the Internet to an array of RHIOs around the state, it is critical that security features, functions, audit trails, identity management and non-repudiation controls are an integral part of this process.

Physicians, patients and the public at large want and believe that the health care industry needs to automate and there is strong support for both EMRs and Personal Health Records (PHRs). Yet this same population, for the most part, does not trust the health care system to use the data properly. This underscores the vital role that trust and security technology play in designing and building the FHIN. Security will play a pivotal role when patients want to securely share their PHI with a caregiver, or access their own PHI through a PHR. CMS has just launched a national program to fund and test a PHR program that will to give individuals access to their prescription history and other medical data, similar to the Blue Cross Blue Shield of Florida activity linked with Availity. So too, the FHIN needs to direct time and effort toward expanding the scope of security features and functions to include consumers and patients in this health-enterprise effort.

In order to embrace security and ensure non-repudiation, it is imperative that access controls and role-based access privileges through identity management tools be addressed. The FHIN security process must insure that only authorized individuals view, access and/or modify aggregate data and/or individual records. The core of the security process must tie to a credentialing process, in order to authenticate individuals and medical professionals. It is critical that security measures be incorporated into the FHIN and that the security processes incorporate real-time audit trails; then we can be assured of building trust and confidence in both patients and physicians.

In January 2006, the Governor's Health Information Infrastructure Advisory Board recommended that the Agency for Health Care Administration form a workgroup to address technical security of the FHIN, the process of authorization, credentialing and authentication of users and the non-repudiation of records. Recommendations from the workgroup will be included in the final draft of this White Paper.

Development of a Master Patient Index and Record Locator Service

*Master Patient Index*

The Master Patient Index can be defined as

> *A software database program that collects a patient's various hospital identification numbers, perhaps from the blood lab, radiology, admission and so on, and keeps them under a single, enterprise-wide identification number.*[12]

The master patient index is sometimes referred to as an Enterprise MPI. For the purposes of discussion in this paper the term MPI is used when referring to a RHIO; the term EMPI is used when referring to the FHIN server's identification of patients. Each RHIO will maintain an MPI for patients seen by providers in the local community area; The FHIN EMPI will mirror all of the RHIO MPIs in a statewide registry that will be updated on a regular basis.

The MPI has been in use for quite some time. Most of the MPIs currently in existence are Enterprise MPIs (EMPIs). Many were designed to work in closed, stand-alone systems, unlike the FHIN, which will be an open system. Statewide and national MPI solutions and their associated RLS solutions are badly needed, especially with the national and statewide pressure for the improvement of healthcare, the desire for longitudinal and lifetime records, and the requirement that systems be interoperable (e.g. HIPAA, ONC, FHIN).

Other countries, including Canada, have started the development of national MPI solutions (e.g. Canadian "client registry"). The need for improved stakeholder identification in the United States was recognized by HIPAA, and some identifiers have been planned for implementation such as the National Provider Identifier. The National Committee on Vital and Health Statistics (NCVHS) has had numerous discussions regarding unique identifiers, including the HIPAA Unique Health Identifier for Individuals (UHI). HIPAA mandates that implementation of each identifier be completed within 24 months after adoption of the final rule for that identifier. However, after numerous discussions on the topic, the United States seems no closer to a solution in the area of unique individual identifiers. Currently the funding for development of a national individual identifier is on hold and, according to the Department of Health and Human Services (HHS), opinions about the unique identifier for individuals are deeply divided.

The current national position leaves HIT initiatives lacking unique individual identification and therefore necessitates MPI solutions that can support multiple concatenated identifiers. The MPI is on the opposite end of the technical spectrum from unique identification. A group in Massachusetts is developing a position on the use of a community MPI. Massachusetts SHARE (Simplifying Healthcare Among Regional Entities) is a regional collaborative initiative operated by the Massachusetts Health Data Consortium. MA-SHARE seeks to promote the inter-

[12] Pamela Tabar, Healthcare Informatics. The Latest Word, January 1998. Retrieved from http://www.healthcare-informatics.com/issues/1998/01_98/glossary.htm on December 10, 2005.

organizational exchange of healthcare data using information technology, standards and administrative simplification, in order to make accurate clinical health information available wherever needed in an efficient, cost-effective and safe manner.

There are several technical solutions for the MPI available. Vendors, such as Initiate have solutions in place, e.g., with *RxHub*. IHE has an integration profile (PIX) that provides a practical, elegant and simple solution for dealing with MPI, which also makes it easier to scale a RHIO as additional subnetworks are added. The PIX integration profile could be a model for federating patient cross-referencing across multiple RHIOs. Health Level Seven (HL7), an ANSI standards body which has been successful in creating lab, pharmacy, and other electronic clinical messaging standards, is also focusing on electronic health records. The HL7 mediation is a software transaction process which is intended to search for and locate patient records in external MPIs. The transactions are designed to send demographic characteristics using HL7 transaction standards to locate and match demographic information in the receiving MPI.

The FHIN may want to have policies in place that require RHIOs to meet a patient identification accuracy metric before becoming part of the FHIN – in order to ensure patient ID "hygiene" before joining a state network.

*Record Locator Service*

While the MPI has been around for many years a newer concept is that of the Record Locator Service. The eHealth Initiative describes the RLS in the following terms:

> *The RLS holds information authorized by the patient about where authorized information can be found, but not the actual information the records may contain. It thus enables a separation, for reasons of security, privacy, and the preservation of the autonomy of the participating entities, of the function of locating authorized records from the function of transferring them to authorized users.*[13]

As this description suggests, the RLS presents identification of records without requiring their central storage. Essentially what is stored in the RLS are metadata, or information about information. The RLS stores enough information to be able to tie a clinical record to an MPI record, as well as the information about where that record is stored. The record locator service is often associated with the decentralized RHIO model, e.g. the original Santa Barbara model. However, the RLS is also required in a centralized model, where data are stored in separate data vaults, as well as a mixed-mode model where some central data are stored but the clinician has the ability to drill down into individual encounters.

A key concept that needs to be dealt with in using an RLS model of any kind is the non-repudiation of records. This is originally a legal term but is also a data term. The concept of non-repudiation in technical terms refers to having an authentication mechanism, such as a digital signature, that allows you to verify, for example, that an e-mail sent from a person actually came from that person and could not have come from any other source. A prime example is the Gold Standard (eMPOWERx) solution mentioned earlier in which a physician writes a prescription for a patient on a PDA, then must enter a password to initiate a digital signature so that later, if it

[13] Working Group on Accurately Linking Information for Health Care Quality and Safety, Markle Foundation. Linking Health Care Information: Proposed Methods for Improving Care and Protecting Privacy. February 2005. Retrieved from http://ccbh.ehealthinitiative.org/communities/community.aspx?Section=105 on December 10, 2005.

needs to be verified, the digital signature can be traced back to the originator and that person cannot repudiate that he was not, in fact, the initiator of the prescription.

Another example of how non-repudiation can relate to electronic records could be the case of a clinician who accesses a RHIO with a decentralized model, that collects data from a variety of sources and collates it into a single health record. Although medical care is delivered on the basis of the information presented to the provider, in most models that collection of data is not permanently stored. If, based on an incorrect match of identifiers, the collated record were to provide inaccurate information which resulted in harm to the patient, giving rise to legal consequences, there would be great interest in reconstructing the collated record that formed the basis of the diagnosis. However, that collated record no longer exists and while it may be possible to go back and reconstruct the record by replicating the search, can it be proven that the new record collated and displayed actually matches the original used to provide clinical care? Under these circumstances, there is no non-repudiation available. This probably remains the single most difficult technical challenge for RHIOs.

The FHIN Network Security Workgroup passed a series of recommendation on audit trails and non-repudiation of data, and has recommended that any audit *include* the following technical elements:

2. (September, 2006): Transaction audits for non-repudiation will be conducted at both FHIN and RHIO levels, based on HIPAA and other industry standards.

   Suggested Audit Trail Requirements:

   a. System Requirements:

      i. Machine start up and shut down times of when audit functions occurred– every time an audit log is included, there is a date and time stamp at beginning and end of file.

      ii. Successful and unsuccessful logins of users.

      iii. IP address of successful and unsuccessful connections.

      iv. Denial of service events.

      v. Anything that adds, modifies or deletes a data object.

      vi. Auditing of all accounts and utilities.

      vii. Any changes to user access – privileges, changes to security levels, etc.

      viii. Switching to another user after logging in.

      ix. Completely separate audit process for the change control process.

      x. Any change to data noted with time stamp based on system.

      xi. Data integrity verification for information that is transmitted or received.

      xii. Audit log of processes when sending data to RHIO.

      xiii. Any changes to security configurations – firewalls, etc.

      xiv. The actual application responsible for executing event in multiple applications.

      xv. Users who cause abnormal events.

b. Clinical level:

   i. Any change to any record that is put into RHIO database is noted – addition, deletion, merging or unmerging of records

c. Process for non-repudiation of records must be worked out.

There have been many discussions on the challenges associated with matching records, and the following is an excerpt from the Federation of American Hospital's response to ONC's Request for Information (RFI) on the NHIN:

> *The ability to accurately and consistently map records and information about a single patient becomes increasingly complex with scale. Traditional computerized clinical systems tend to focus on specific areas of functionality. In the new world of the electronic health record and patient health record there will be a requirement to bring together information from a variety of systems, often across providers and sectors in the healthcare industry.*
>
> *The experience even within a single healthcare provider is that matching of patient records is far more complex than it may appear. Factors that must be taken into consideration include:*
>
> - *Patients themselves often enter information incorrectly on forms*
> - *The input of information into computerized systems is still done by people (who can make errors) such as duplicate registrations, data entry errors, etc.*
> - *People move into and out of geographic areas*
> - *That given a population of 300 million people the potential for people to have the same names is surprisingly high*
> - *That people may use different variations on their own names (Tom Jones, Tommy Jones, Thomas Jones), and may change names due to marriage, divorce or adoption and many other factors.*[14]

While many of these factors are amplified in a national setting, they are nonetheless still valid at both a regional and a state level. Risks associated with an MPI or RLS include both the under-matching of records, potentially leaving out a vital piece of clinical information, and the overmatching of records where data from two patients are joined together. Ultimately decisions will need to be made as to who is responsible for any inaccuracies or mismatches.

From the FHIN perspective, what is key is that a common set of identifiers be used across RHIOs for patient identification. A common phrase used in the IT industry is sub-optimization, the process whereby as system is optimized for maximum benefit internally at the detriment of interoperability and integration with other systems. Clinical IT is well-documented as being sub-optimized, at a system, entity and state level. The risk in allowing disparate schema for

[14] Federation of American Hospitals. Response to Request for Information, January 18, 2005. Retrieved from http://www.fahs.com/issues/comment_letters/2005/CL%201.18.05%20BrailerRFI.pdf on December 10, 2005.

identification of patients to be used for different RHIOs is that a new level of sub-optimization is created that hinders interoperability between RHIOs.

Following the recommendation of the Governor's Health Information Infrastructure Advisory board, the Agency for Health Care Administration will publish a RFI in the spring of 2006 to seek input into the best approach to developing an EMPI and RLS for the FHIN. Vendor responses will be analyzed and will be used to further develop the requirements of a statewide EMPI. A future Request for Proposal may result from this RFI.

Privacy and Confidentiality of Patient Records

At the core of the RHIO and FHIN discussion lie issues around confidentiality and privacy. Patients' rights groups make a strong case for the right of the patient not only to control who has the right to view information stored in a medical history, but also what information should be allowed to be shared with regard to the medical history. At the outset the FHIN needs to design the mechanisms to allow for effective and cost-effective patient control of medical information. Caution needs to be exercised in designing an IT infrastructure, that the costs of implementing some of the proposals being recommended by different groups are clearly understood.

The fundamental difference between privacy and confidentiality lies in the focus of the data being dealt with. Medical privacy is about the human desire to control what information is shared about a person's health status. Confidentiality is about how the danger is handled once the patient and the person holding the data enter into a agreement, including the safeguard required to ensure that the data are only provided in an appropriate manner to those persons with the authorization to view the data. More simply, privacy is about people while confidentiality is about systems, and these differences are recognized in federal law.

At the one extreme of the debate around privacy and confidentiality are models which would require that no data be shared unless a patient explicitly opts-in and selects to share the data for a given visit. This is different from a patient who may simply decide to opt-out entirely from a RHIO or from the FHIN.

The middle ground most commonly covered in this debate suggests an opt-out model, whereby a patient would still have the rights to determine what pieces of information were included in a RHIO, or to exclude themselves completely, but in choosing to do so would have to explicitly opt-out from the data-sharing process.

The other extreme of the debate points out that HIPAA already has safeguards and processes in place to cover patient privacy, and therefore shifts the focus onto confidentiality. Within this model under HIPAA there are already preexisting conditions under which data may be shared between business entities, normally covered under what is called a business associates agreement (BAA). Where a BAA does exist between two entities, explicit patient consent is not required to share data if it can be shown that a valid business function is being performed by the organization receiving data behalf of the provider.

Even within these models there are variations. Some patients' groups argue that not only should a patient be allowed to select which visit is included in a shared medical record, but within each record clinical data categorization should be created which would separate sensitive data from

regular clinical data, the most common example being AIDS and information relating to mental health.

While recognizing the validity of the patients' rights to control their own clinical data, it is often pointed out that to allow patients to opt-out from sharing data in many cases would work against the most often cited reasons for the creation of RHIOs, and the FHIN. In the following examples, problems related to using the opt-out method are apparent:

- One of the most common reasons for the creation of a RHIO is the desire to share data between emergency departments of hospitals in order to detect what are called "frequent fliers," patients who use emergency departments for primary clinical care on an ongoing basis, or patients who move from emergency department to emergency department seeking narcotic drugs. It may be argued that if a patient can elect not to include specific emergency department visits in the shared data the specific aim of information exchange, often cited in the financial cases for the creation of the FHIN, would be compromised. Also, these very patients are the ones most likely to opt out.

- Likewise one of the major drivers behind the creation of the FHIN, and a key cornerstone of RHIO financial sustainability, is the ability to monitor and share test results in order to eliminate unnecessary duplicate testing. Once again if a patient can choose not to allow certain clinical encounters to be shared the number of duplicate tests eliminated might be reduced, effectively reducing the financial long-term sustainability of the RHIO model.

- Within the strategic framework laid out by HHS in 2004, one of the primary aims for the creation of the NHIN was the sharing of research data for use in approval of drugs by the FDA and for other research. Once again if data are not shared completely within the RHIOs, and the RHIOs in turn become the basis for the creation of limited datasets for research purposes, the validity of the data available for research is called into question.

- One of the primary drivers behind the creation of the NHIN was the ability to create an aggregate data system for detection of bio-terrorism events and other clinical events. These systems, already being implemented in various forms across the United States, would be crucial to early detection of anthrax, smallpox, or avian flu. In the event of patients being able to opt-out from information being included in the RHIO datasets, these datasets would in turn not be able to provide data to the CDC for this type of event detection, placing the burden back on healthcare providers.

- For these reasons, while fully recognizing patients' rights to be able to control their own clinical information, the authors of this paper would caution against the adoption of opt-out models for RHIOs.

In addition to the reasons listed above there is another key financial criterion which would be affected by the inclusion of opt-in models. The RHIO, and in turn the FHIN, are built on data sourced from primary physicians, clinics, hospitals, and a variety of other sources. Investment in clinical IT, for many of these entities, is a major and ongoing investment. If one were to take the model of the patients being required to opt-out to a RHIO at the point of registration, there as an immediate ripple down effect.

Very few (if any) EMR systems have the necessary fields to identify whether or not the patient has chosen to share the information with the RHIO. Likewise, very few systems have the ability to identify "more confidential" or "less confidential" data, and to be able to separate them out in terms of supplying data to a central infrastructure, for example mental health versus other clinical information.

As a result, the source IT systems would have to be modified in order to accommodate the needs of the opt-out model. Additionally, due to lack of coordination at the national level with regard to these models, vendors, such as Cerner, Meditech and Epic, may be required to provide different levels of modification for different RHIOs. The cost of modifying the systems would be born by the vendors, and by the providers who would have to implement these as upgrade projects. If the integration into RHIOs is to remain a voluntary process the associated cost and time may work against adoption of the RHIO concept.

Additionally it needs to be noted that the actual registration process would be changed. Staff would have to be retrained to cope with the new registration process, forms would need to be printed and training would need to be provided to ensure that questions by patients would be answered in uniform manner. In short, what seems like a reasonable and relatively easy requirement to implement does in fact have associated with it considerable information technology, products, project, staff and implementation cost.

For these reasons the authors of this paper would recommend that consideration be given to alternative systems to ensure patient rights, such as the adoption of a personal identification number (PIN) model external to both the source systems and the RHIO. Within this model a system would be written which would allow patients to be registered containing enough demographic information to identify themselves, against which a patient could choose a PIN, similar to systems used for online banking. The database housing the patient information and patient-held PIN, would be housed in a highly secure central location, with redundancy and disaster recovery implemented as part of the design.

When a patient sees a clinician at the local RHIO level, the patient would provide the clinician with the PIN number if she wishes to have the clinician view her health record. The physician could provide a touchpad, for example, so the patient could key in the PIN. The clinician would first authenticate with the local RHIO, which would then send a request to the central server containing the patients demographic information and PIN that has been provided. The central server will return to the RHIO a simple "yes" or "no," either the PIN matches the patient or it does not. In the event of a match the clinician is allowed to continue on and view the patient record, in the event of a mismatch access the request is denied. In the event of an emergency, provisions for a physician to "break the glass" to access a patient's information without the PIN would also have to be in place.

Each time that a request is made to the central server, the requesting clinician's details and the dates and time of the request are stored centrally at the PIN server for future audit purposes.

The patient should be able to access the server through a secure portal and perform a number of administrative functions. These would include completely changing the PIN if patients decide they wish to opt-out entirely from the statewide system. An alternative would be to request a list of all the clinicians who have requested the health information using the PIN, and to be able to

selectively choose not to allow any one provider continued access to the shared health information, even if the provider held the correct PIN.

Using this model under a business associate agreement patient records would automatically be shared, however patients would retain the right and the ability to determine who was able to see their health record, and selectively refuse access, while still allowing the information to be made available for the vital tasks of research, event detection, and fraud detection.

The model is not without problems. While widely used within the banking industry, it needs to be noted that within the financial model an account is always created before a patient is allowed to go in and register for a PIN. In order to be able to register, the patient must provide a variety of data, including personal information and the account number. Concern could quite rightly be raised that somebody could register under a false name, attempting to use the system to gain health care entitled to somebody else.

A number of steps need to be taken to ensure that a false registration does not occur. While patients could still be allowed to self register through the public portal (effectively creating a record), the record would need to be placed in a pending status until the first health care encounter has occurred. Positive physical identification would be required at the time of the first clinical encounter which, in conjunction with the PIN, would be used to validate that the record registered was legal and move it to full status. In addition, statewide guidelines would be required that positive identification and a physical copy of any medical insurance card were provided at each encounter, to obviate the potential situation where a patient claims to have left the identification at home and urges the medical provider to use the PIN as a form of identification.

Finally it needs to be noted that not all populations have universal access to the Internet, and even within the populations who do have such access, it cannot be assumed that everyone has the skill set required to navigate an Internet portal. As a result, systems would need to be put in place similar to those provided by the banking industry, whereby a touch tone telephone could be used to dial into the system, create and change a PIN, and retrieve recent encounters. This model is by no means the only one available to ensure patient rights when sharing health care information. It is merely an example of how alternatives can be found which may not have the overhead and cost associated with the traditionally discussed opt-in and opt-out models.

In January 2006, the Governor's Health Information Infrastructure Advisory Board recommended that the Agency for Health Care Administration form a workgroup to address patient rights issues. This workgroup will discuss patient privacy in the spring of 2006 and recommendations from the workgroup will be included in the final draft of this White Paper.

## VII. Recommendations

Central Authority for Technical Standards

The state of Florida should endorse and create an independent, neutral, central, not-for-profit organization to set standards and certify RHIOs to meet the FHIN policy and technical requirements. The FHIN should leverage existing standards wherever possible. The FHIN will extend web services and content standards to provide state-level reliability and security specifications, and to model the key inter-RHIO processes for health care. The FHIN will work closely with standards recommendations of the AHIC and the NHIN.

- In order to achieve the goals as stated for the FHIN in the timeframe allotted and for the continued viability of the network, the FHIN should have the authority to adopt standards, and to announce and plan for the deprecation of existing standards. This should be an ongoing technical strategy of the governing body of FHIN. Sunset and maintenance rules must be created and adhered to, perhaps tying access and/or rates with established compliance timeframes. A continuously rolling 3-5 year plan should be published with achievable milestones.

- The early phases of the state network should focus primarily on business-to-business (B2B) infrastructure, including perhaps most importantly among providers. Consumer interaction and views to data should be limited until RHIO infrastructures develop. This will reduce the complexity and mitigate the security and privacy issues of information exchange significantly. The state network should ensure connectivity, access, and interoperability to the business constituents of the health care community prior to affording interoperability to consumers through a personal health record.

- Financing and access to the FHIN should be based on vested interest and utilization by the health care supply chain constituents in the state. The government, payor, provider, vendor, and supplier sectors will share initial funding. Ongoing financing should be equitable across states and should be based on current market transaction rates or another equitable method, for example, charging per physician per month or per member per month (note that the calculated charge does not necessary equate to who pays). The FHIN should have the option and flexibility to have a public, private, or combination offering that meets the dynamics of the marketplace in the state.

Network Security

Clinicians shall connect to the RHIOs, and RHIOs shall connect to the FHIN using a secure and encrypted communication channel that meets standards as articulated in the HIPAA Security Rule and consistent with provisions in state statutes. Consideration should be given to the use of secure sockets layer (SSL), public key infrastructure (PKI) and virtual private network (VPN) technologies. RHIOs shall be able to respond to a specified set of HL7 XML requests, and shall address the state server using the same mechanism. X12 capabilities should also be incorporated so that claim attachments can be enabled as an efficient method for clinical data exchange. No web-services should be addressable using the public Internet.

- Public access to patient portals should follow the guidelines laid out for the banking sector, including encryption standards and two-factor authentication.
- If a Private MAN is used for communication, the RHIO (or state server in the case of a statewide MAN) shall be responsible for auditing the security of the MAN and for maintaining an up to date list of all connections to the MAN.
- A common set of vocabulary and coding standards shall be adopted across the state to facilitate interoperability, quality reporting and bio-surveillance. All standards adopted will be vetted at the outset against proposals from CMS, HHS and AHRQ, and shall be reviewed against emerging national trends on a bi-annual basis.

In addition to these recommendations, the following recommendations were made by the FHIN Network Security workgroup:

- Motion (August, 2006): Incorporate by reference the National Institute of Standards and Technology (NIST) summary. Bullet points to guide RHIOs in discussion.
- Motion (September, 2006): Authentication of clinicians entails the following criteria:
  - Use of digital signatures in two factor authentication.
  - Authentication takes place at the FHIN (credential check) and then the RHIO. Once user is authenticated at both levels, then all transactions are trusted after FHIN authentication.
  - Role-based authentication.

3. Technical Infrastructure Requirements of the FHIN

No central standards should be set for hardware and software, however a minimum set of non-functional requirements needs to be specified by the FHIN and adhered to by each RHIO in order to be certified. These include:

- Availability: Any the system that will be used for clinical care should have availability above 96%, 24/7.
- Redundancy: All systems should have no single point of failure.
- Scalability: Systems should be designed in such a way that sufficient system overhead is available to handle a specified percent of unusual activity.
- Backup: Backup and restore procedures shall be implemented in accordance with industry standards, including offsite storage.
- Disaster recovery: All systems will provide a disaster recovery plan with a site outside of the immediate region, and shall be tested at least once per year.
- Security: All systems will be housed in secure locations, including a DMZ for all public facing servers. All publicly available systems will be tested annually for vulnerabilities.
- Synchronous versus Asynchronous Communications: All communications from an end user to the local RHIO should be synchronous, whereas communications between the RHIO and

the FHIN server and to other RHIOs should be asynchronous. When a physician connects to a local RHIO, the local information stored within the RHIO database would be provided for any given patient on a synchronous basis. Searches for information outside of the regional system will be done asynchronously, and would be displayed as links when it becomes available. This may mean that local summary information for a patient is displayed within five seconds, while a separate part of the user interface is reserved to display links to other information, which may be available to the physician as the information is identified and the links sent back to the local RHIO.

Authentication of Users

It was originally recommended that end-user authentication and authorization should be handled at a regional or RHIO level, with a trust relationship set up between RHIOs and the state server. The state server shall act as a broker of all transactions among individual entities such as RHIOS, state agency databases or other sources of health care information. This would ensure that the authentication of clinicians and other end users does not need to occur at every single step of the data request and process.

With reference to the recommendation above, however, a recommendation was made by the FHIN Network Security Workgroup that the FHIN is responsible for credentialing all physicians who want to join a RHIO, or connect directly to the FHIN. Additionally it was recommended that authentication takes place at the FHIN (credential check) and then the RHIO. Once the user is authenticated at both levels, then all transactions are trusted after FHIN authentication.

It needs to be noted that this is a variance from the original white paper recommendation listed above, and is not how the RHIOs are currently being designed, as the FHIN infrastructure is not currently in place.

If this recommendation is carried forward consideration will need to be given to how the RHIO will handle an event where connectivity to the FHIN server is lost, while still allowing local clinician access. At a minimum an audit log should be maintained indicating that the audit event was unable to be completed. Consideration should be given to caching the last credential call and using that as the basis for a credentialing decision in the event of connectivity being lost.

- Detailed logging of all requests to the FHIN server, or between RHIOs and other entities must be kept at all times, preferably both by the requesting entity and by the requested entity.

Patient Consent

The technical design of the FHIN and RHIOs needs to be defined in such a way that patients have control over the medical information stored within their medical record, while not creating a process that is overly complex for the patient and provider, or that drives cost up to unacceptable levels for the overall solution. Patients should have the right to determine who is able to view their shared information, revoke the right if they choose to do so, request an audit of who has been viewing their information, and be notified of any event that breaks these rights.

For these reasons the authors of this paper would recommend that consideration be given to alternative systems to ensure patient rights, such as the adoption of a personal identification number.

- It is recommended that a statewide patient authorization system be investigated, possibly using a patient controlled PIN which is externalized to the RHIOs or source systems. This will allow the patient to control exactly who has access to their identifiable health information, while requiring minimum changes to existing systems.
- FHIN should explore the feasibility of a web portal that patients could access directly to manage access policies themselves, with an alternate mechanism by phone/mail for those without Internet access. For these patients, when a hard copy is mailed to them, they can edit and return it, and the data are entered by an authorized employee. This option would be more cumbersome than the online option and therefore would not be over-utilized.
- Caution should be exercised in implementing opt-in or opt-out models at the provider level, as this will require changes to both the registration process and the underlying provider systems, driving up incremental costs. It is recommended to not allow patient opt-in and opt-out scenarios at a RHIO level, but rather that a Business Associates Agreement in accordance with HIPAA should be in place that allows for sharing of data.
- Medical staff should, when circumstances require, have the right to "break the glass" and view a patients medical record for medical necessity, with the appropriate logging of such events and patient notification after the fact.

The recommendations of the FHIN Network Security Workgroup with regard to “breaking the glass” are:

- Motion (September, 2006): Notification of patient that records have been released in an emergency, upon agreement of two physicians to “break the glass,”
  - Passwords for both physicians are required.
  - The event of the “glass being broken” needs to be tracked in an audit trail with all of the necessary precautions that it cannot be modified at later stage.
  - A physical letter of notification, with no PHI, sent to patient within 14 days of event to last known physical mailing address.
  - A solution should be explored that maintains the rights entrenched in HIPAA and enforces those while not creating unnecessary additional burdens in implementing solution.

Master Patient Index

A common set of fields should be identified and used by all RHIOs for patient identification. These should include first and last names, phone number, date of birth, city or location of birth, or a personal identification number (PIN).

Minimal Clinical Dataset

The decision to implement a centralized, federated or mixed mode RHIO architecture should not be dictated by the FHIN. However, each RHIO should create a minimal clinical dataset of priority data fields culled from patient records, to be held on the RHIO server for immediate downloading to the local physician upon request.

- It was the recommendation of the authors of the white paper that the State of Florida seriously consider the adoption of the continuity of care record, or a subset of the continuity of care record, as the basis for partially central storage in a mixed mode model. Standards for a minimal data set to be collected and displayed by RHIOs should be established by the FHIN to ensure interoperability across the state. To this end a Minimal Clinical Subset Workgroup was formed consisting of various clinical and quality experts, and the recommendations of that group are listed elsewhere in this paper. The subset of data was drawn up using the principles that:
    - The data set should be in accordance with harmonized CCR/CDA standards, and should take into account any data sets defined by through HHS, ONC and AHIC.
    - The data set will not be comprehensive and should be extensible by any RHIO.

## VIII. A Strategic Timetable for the FHIN

The Florida Health Information Network (FHIN) represents a bold vision for the future of health care in Florida. This White Paper outlines the key issues necessary for full implementation of the FHIN, but does so in terms of the final outcomes, without discussing the steps that need to be taken over time to achieve its goals. Building out the FHIN will take several years and will require a clear cut timetable to specify technical priorities such as developing the FHIN server, incorporating the master patient index and record locator services and integrating state level and provider-generated claims databases. Additionally, the development of regional health information organizations (RHIOs) across the state will also occur over a period of time. The FHIN will need to develop business agreements with the RHIOs, create connections with them, integrate their master patient indexes and ensure security for network communications.

In its first year, the FHIN will need to develop its organizational and administrative structure to establish leadership for developing a health information network. The next step will be to build the physical infrastructure component of the FHIN servers, install the master patient index and record locator service and develop the FHIN web portal, presentation screens and web services interfaces that will let the FHIN connect to the RHIOs. An important goal of the FHIN is to establish standards to facilitate communications among RHIOs. In addition, the FHIN will enable physicians across the state to access state level or provider-generated claims data via the FHIN. The FHIN will develop systems for accessing the health care providers State Center for Health Statistics historical patient encounter datasets, the Department of Health immunization database and provider-generated claims data. Each of these datasets will become available to authorized users through the FHIN web portal.

In its second year the FHIN will begin connecting the RHIOs that are emerging across Florida. At present there are three health information exchange projects working under FHIN grants building the local infrastructure to exchange medical records. In the fiscal year 2006-2007 there could be eight or nine health information exchange projects working under FHIN grants. This step will require testing of web services interfaces, development of update schedules for keeping record registries current, and far-reaching quality assurance to ensure that the correct records are returned when queries are sent. The second year of the FHIN will also be a year of outreach to physicians to encourage investment in electronic health record systems, to hospitals and clinics to integrate their electronic medical record systems, and to communities that have not come together to form a RHIO.

## IX FHIN Development Budget

**Budget Estimates for Core Functions of the Florida Health Information Network**

**Based on Recommendations from the FHIN Budget Workgroup**

| **Operations and Administration** | | **2007-08 ($9.4M)** | **2008-09 ($8.7M)** | **2009-10 ($7.7M)** |
|---|---|---|---|---|
| Executive Director | Chief Administrator for the FHIN Corporation | $140,333 | $140,333 | $140,333 |
| Chief Technical Officer (3) | Technical director and intermediary with vendors | $287,667 | $287,667 | $287,667 |
| Administrative Staff (6) | Administrative support for FHIN Corporation | $664,000 | $664,000 | $664,000 |
| Legal Consultant (2) | Legal retainer for contracts, BAA, etc. | $220,000 | $220,000 | $220,000 |
| Travel | Travel in Florida and USA | $60,000 | $60,000 | $60,000 |
| | **Subtotal Operations Administration** | **$1,372,000** | **$1,372,000** | **$1,372,000** |
| **Core Functions of the FHIN** | | | | |
| Enterprise Master Patient Index | Patient identification using a limited set of identifiers | $1,750,000 | $1,000,000 | $600,000 |
| Record Locator Service | Record location and pointer for accessing record | $2,250,000 | $1,000,000 | $600,000 |
| Data exchange interface with RHIOs | Web services interface for file transfer | $350,000 | $480,000 | $480,000 |
| Registration/certification | Qualifying criteria for access to the FHIN | $400,000 | $100,000 | $100,000 |
| Authentication | Identification of qualified user | $450,000 | $100,000 | $100,000 |
| Secure communications | Secure messaging using encryption | $550,000 | $30,000 | $0 |
| Audit trail and reporting for non-repudiation | Risk mitigation, fraud prevention | $325,000 | $30,000 | $30,000 |
| Disaster recovery | Secure backup of data | $220,000 | $20,000 | $20,000 |
| Broadband Connectivity | Broadband connection to the Internet | $150,000 | $200,000 | $200,000 |
| | **Subtotal Core Functions** | $6,445,000 | $2,960,000 | $2,130,000 |

| | | | | |
|---|---|---|---|---|
| **Core Services of the FHIN** | | | | |
| E-Prescribing | Electronic prescribing system for physicians | $115,000 | $1,500,000 | $1,500,000 |
| Interfaces with State Agencies | Interfaces with state agencies for health care data access | $250,000 | $300,000 | $300,000 |
| Interfaces with Pharmacy Network | Interface for delivery of prescription information, e-prescribing, medication management | $120,000 | $200,000 | $200,000 |
| Interfaces with Laboratories | Interface for delivery of lab reports; interface for delivery of prescription information, e-prescribing, medication management | $130,000 | $200,000 | $200,000 |
| Minimal Clinical Dataset | Patient medical summary for physicians connecting directly to the FHIN | $200,000 | $250,000 | $250,000 |
| EMR-Lite | Interactive web portal that supports display of FHIN MCDS information and limited input to the MCDS for physicians connecting directly to the FHIN | $150,000 | $500,000 | $500,000 |
| PHR-Lite | Interactive web portal that supports display of FHIN MCDS information and limited input to the MCDS for consumers | $2,000 | $800,000 | $600,000 |
| | **Subtotal Core Services** | $967,000 | $3,750,000 | $3,550,000 |
| | **Subtotal Core Functions and Services** | **$7,412,000** | **$6,710,000** | **$5,680,000** |
| **Communication and Training** | | | | |
| Marketing and Communications | Developing a marketing plan, physician and consumer outreach | $330,000 | $330,000 | $348,000 |
| Physician Training Program | Develop and implement a training program for phsycians on integrating EMR systems in their workflow | $286,000 | $288,000 | $300,000 |
| | **Subtotal Communication and Training** | **$616,000** | **$618,000** | **$648,000** |
| | **Totals** | **$9,400,000** | **$8,700,000** | **$7,700,000** |

## X Glossary

| Acronym | Full Name |
|---|---|
| 24/7 | Available twenty-four hours per day seven days a week |
| ACC | American College of Cardiology |
| ACP | American College of Physicians |
| AHCA | Florida Agency for Healthcare Administration |
| AHIC | American Health Information Community |
| AHRQ | Agency for Healthcare Research and Quality |
| ANSI | American National Standards Institute |
| ASC | Accredited Standards Committee |
| B2B | Business-to-business |
| BAA | Business Associate Agreement |
| CalRHIO | California Regional Health Information Organization |
| CCR | ASTM Continuity of Care Record |
| CDA | HL7 Clinical Data Architecture |
| CMS | Centers for Medicare and Medicaid Services |
| CRS | Care Record Summary |
| CT scan | Computed Tomography scan |
| DMZ | Demilitarized Zone |
| DOH | Florida Department of Health |
| EDI | Electronic data interchange |
| EHR | Electronic health record |
| EHRVA | Electronic Health Record Vendors Association |
| EMPI | Enterprise Master Patient Index |
| EMR | Electronic medical record |
| ePHI | Electronic patient health information |
| FHIN | Florida Health Information Network |
| GHIIAB | Governor's Health Information Infrastructure Advisory Board |
| HHS | Department of Health and Human Services |
| HIMMS | Healthcare Information and Management Systems Society |
| HIN | Health information network |
| HIPAA | Health Insurance Portability and Accountability Act |
| HIT | Health information technology |
| HL7 | Health Level 7 |
| IHE | Integrating the Healthcare Enterprise |
| IHIE | Indiana Health Information Exchange |
| IT | Information Technology |

| Acronym | Full Name |
|---|---|
| MAN | Metropolitan Area Network |
| MPI | Master Patient Index |
| MRI | Magnetic resonance imaging |
| NCVHS | National Committee on Vital and Health Statistics |
| NHII | National Health Information Infrastructure |
| NHIN | Nationwide Health Information Network |
| NHS | National Health System, UK |
| ONC | Office of the National Coordinator of Health Information Technology |
| PACS | Picture Archiving Communications System |
| PGCR | Provider-generated claims record |
| PDA | Personal digital assistant |
| PHI | Protected health information |
| PHR | Personal Health Record |
| PKI | Public Key Infrastructure |
| PIN | Personal Identification Number |
| RFI | Request for Information |
| RHIO | Regional Health Information Organization |
| RLS | Record Locator Service |
| RSNA | Radiological Society of North America |
| SHOTS | State Health Online Tracking System |
| SSL | Secure Sockets Layer |
| TCP/IP | Transmission Control Protocol/Internet Protocol |
| UHI | Unique Health Identifier for Individuals |
| UHIN | Utah Health Information Network |
| VA | U.S. Department of Veterans Affairs |
| VPN | Virtual Private Network |
| XML | Extensible markup language |
| X12 | Standard for electronic data interchange |

This page intentionally left blank.

# Appendix A

## Contributing Authors and Reviewers

This page intentionally left blank.

**Florida Health Information Network**

**Architectural Considerations for State Infrastructure**

**White Paper Contributing Authors:**

Peter Greaves
Hospital Corporation of America Inc. and
Governor's Health Information Infrastructure
Advisory Board

Christopher Sullivan Ph.D.
Agency for Health Care Administration

Huy Nguyen M.D.
Cogon Systems Inc.

Jon McBride
Availity Inc.

Lisa Rawlins
Agency for Health Care Administration

Jim Kragh
Good Health Network Inc.

Mary Moewe
Hospital Corporation of America Inc.

Patrick Rooney
Cogon Systems Inc.

Bob David
TECHSOFT Inc.

**White Paper Reviewers:**

Blair Butterfield
GE Healthcare Integrated IT Solutions

Lester Chan
California Office of HIPAA
Implementation

John W. Collins
Agency for Health Care Administration

Ron Fucci
JaxCare, Inc.

Mark Gerszewski
Bay Systems, Inc.

Mary Griskewicz
GE Healthcare Integrated IT Solutions

Steve Halleck
Affiliated Computer Systems, Inc.

Michael Heekin, Chair
Governor's Health Information
Infrastructure Advisory Board

Kevin Kearns
Health Choice Network

Jeffrey Landry
Health Care IT Consultant

Dick Rauber
GE Healthcare Integrated IT Solutions

Michael Solomon
GE Healthcare Integrated IT Solutions

Carolyn Turner
Agency for Health Care Administration

Hugh Zettel
GE Healthcare Integrated IT Solutions

This page intentionally left blank.

# Appendix B

## FHIN Minimal Clinical Dataset Workgroup

## Data Fields Recommended for Minimal Dataset

This page intentionally left blank.

## FHIN White Paper Minimal Clinical Dataset Workgroup

During the January 12, 2006, board meeting of the Governor's Health Information Infrastructure Advisory Board, Peter Greaves presented the draft Florida Health Information Network (FHIN) White Paper to the board members. One of the recommendations in the White Paper was that each Regional Health Information Organization (RHIO) store a minimal data set of medical records on the RHIO server to provide clinicians with an immediate summary of the most important patient records when they query the FHIN. The board members recommended that a workgroup be formed to discuss the most appropriate data fields to be stored on the RHIO servers, and to return a recommendation to the Board for inclusion in the White Paper. Mr. Peter Greaves of the Governor's Advisory Board chaired the workgroup.

The workgroup met between April and August 2006. The workgroup was tasked with the job of recommending a set of data elements that would make up a minimal clinical dataset on the RHIO servers. Member of the workgroup included:

### FHIN Minimal Clinical Dataset Workgroup Members

Mr. Peter Greaves BA HDE DSE
Senior Enterprise Architect
HCA Information Technology & Services

Dr. Phillip Brown, M.D.
Medical Director of HCA-CCMN
Hospital Corporation of America

Mr. Ron Fucci
MIS Project Manager
JaxCare, Inc.

Mr. Paul Gionfriddo
Executive Director
Palm Beach County Community Health Alliance

Dr. Dan Kaelin, MD
Chair, BBRHIO
Vascular Surgery Associates

Ms. Mary L. Moewe, MT(ASCP), MS, CHE, PMP
Director, Clinical Solutions
IT Strategy & Planning,
HCA Information Technology and Services

Dr. Huy Nguyen, MD
CEO
Cogon Systems, Inc.

Dr. Lisa Simpson, MD
National Director, Child Health Policy
National Initiative for Children's Healthcare Quality

Dr. Bernd Wollschlaeger, MD
Medical Director
Aventura Family Health Center

Dr. William M. Sappenfield, MD, MPH
State MCH Epidemiologist,
Division of Family Health Services
Florida Department of Health

Dr. Dennis F. Saver, M.D.
Chairman of the Board
FAFP

Dr. Mel Seek, MD
Physician
South Pine Medical Park

Dr. Ian Nathanson, M.D.
Director,
Nemours Clinical Management Team
Nemours

# Appendix C

## FHIN White Paper Network Security Workgroup Perspectives in Security

This page intentionally left blank.

## FHIN White Paper Network Security Workgroup

During the January 12, 2006, board meeting of the Governor's Health Information Infrastructure Advisory Board, Peter Greaves presented the draft Florida Health Information Network (FHIN) White Paper to the board members. One of the issues addressed in the White Paper was that of network security. The board members recommended that a workgroup be formed to discuss network security issues, and to return a recommendation to the Board for inclusion in the White Paper. Mr. Peter Greaves of the Governor's Advisory Board chaired the group. The workgroup held meetings from May to September 2006.

The Network Security Workgroup was tasked with addressing the following issues:

- Requirements for developing a secure FHIN server and network
- Assessing HIPAA requirements for the FHIN network
- Credentialing and authentication of users
- Authorization of users and appropriate access
- Credentialing of office staff with position designation.
- Transaction auditing for the non-repudiation of records
- Minimum standards for data backup and disaster recovery so that the state switch sees those data and so that each RHIO is responsible for its base of data.

Members of the FHIN Network Security Workgroup included:

**FHIN Network Security Members**

| | |
|---|---|
| Allen Byington<br>CEO<br>Electronet Intermedia Consulting | Bob David<br>Analyst<br>TechSoft |
| Mike DeShazo<br>Security Consultant<br>Computer Training and Consulting | Mark Gerszewski<br>CIO<br>Bay Systems |
| Bryan Graves<br>Information Security Architect<br>HCA Information Technology & Services | Peter Greaves<br>Senior Enterprise Architect<br>HCA Information Technology & Services |
| Jim Kragh<br>President/CEO<br>Good Health Network Inc. | Jeffrey Landry<br>Health Care Consultant<br>Self Employed |
| Wuhong Li<br>Senior VP Application Development<br>Gold Standard | Jon McBride<br>Chief Technology Officer<br>Availity |

Dick Rauber, FHIMSS, CPHIMS
Sr. Account Executive
Integrated IT Solutions, GE Healthcare

Timothy Rearick
Program Management Consultant
Integrated Computer Solutions, Inc.

Alejandro Romillo
CIO
Health Choice Network, Inc.

Christi Rushnell
CIO
Health First

Srivaths Srinivasan
Manager Research IT Systems
Moffitt Cancer Center

Joseph Wagner
VP & CIO
North Broward Hospital District