Federation of American Hospitals

January 18, 2005

Dr. David Brailer, M.D., Ph.D.
Office of the National Coordinator Health Information Technology
Department of Health and Human Services
Attention: NHIN RFI Responses
Hubert H. Humphrey Building, Room 517D
200 Independence Avenue S.W.
Washington, DC 20201

Re: Response to Request for Information

Dear Dr. Brailer:

The Federation of American Hospitals ("Federation"), the national representative of privately owned and managed community hospitals and health systems throughout the United States, is pleased to respond to your request for information as published in the Federal Register on November 15, 2004. We appreciate the opportunity to provide input to you on this important issue.

At the outset, we thank HHS for its efforts in examining the complex issues related to a National Healthcare Information Infrastructure (NHII) and seeking early input. FAH members are committed to the broad aims of the NHII that include the reduction of costs, providing clinical information to the clinician when and where needed, providing data for research purposes, providing a patient portal to empower the patient to take greater control of their own healthcare, and bio-terrorism and clinical event detection.

Our response covers six areas worthy of particular focus from a provider perspective and drills down into key factors for each of these areas. The areas of focus are:

- the potential need for different architectures;
- the need for simplicity in architecting and implementing solutions;
- the need for national standards in governing local solutions;
- the implications of HIPAA;
- the consideration of costs and financial impact, and
- the technical feasibility of certain key areas of functionality.

Where possible, we have tied our response to a specific question(s).

Different Architectures for Different Requirements

We see at least three broad objectives for the NHIN:
(1) the collection of clinical data for an Electronic Health Record (EHR) and a Personal Health Record (PHR);
(2) the collection of de-identified clinical data for research;
(3) the collection of clinical data for bio-terrorism detection and the subsequent ability to access into identifiable data once a potential bio-terrorism event has been identified. It is our view that many of the proposed Local Healthcare Information Infrastructures (LHIIs) or Regional Healthcare Organization Infrastructures (RHIOs) solutions appear to only support part of the NHII objectives. Based on the different requirements for the objectives, we envision the need for three different architectures to support the requirements.

The first two objectives as outlined above are easier to conceptualize, based on existing operational and data warehouse models, although we wish to emphasize caution in assuming one architecture could meet both needs. For example, some Care Data Exchanges (CDE), such as the Santa Barbara model, aim to create peer-to-peer regional networks that allow a clinician to query a central portal to gain a centralized view of a patient's medical record . The CDE, in turn, queries all the source systems of participating organizations. A portal may also be provided to the patient. In this design, the CDEs explicitly do not retain the collated data in a central location and there is no central database of actual medical records. The absence of a centralized database may make the aims of bio-terrorism detection and/or collation of data for research purposes harder to achieve. Likewise there are RHIOs which aim to create central repositories of data for research and analysis purposes, but do not intend to provide either the clinical or patient portal.

The third objective, bio-terrorism detection, creates unique architectural challenges which we feel will require special attention. In order to perform bio-terrorism event detection, rules will need to be in place that look for patterns in diagnosis and treatment. If these were to occur in a decentralized model, such as the CDE outlined above, one of two things will need to occur:

1. Rules will need to be set in each and every system looking for patterns and events. Criteria developed and criteria set by the CDC, and other organizations, would require immediate notification of events. The cost and complexity of putting such a set of rules in place for every healthcare system in the country would drive up cost, complicate maintenance and operations, and create a complex administrative structure.
2. Data would need to be sent in near real-time to centralized databases where rules and pattern detection could then run on events as they arrive, which in turn allows

> them to be flagged. This would require the creation of an unspecified number of central databases, drive changes in all source systems to allow for the 'double-writing' of events, and require considerable bandwidth for transmission of data. The transport mechanism for the data would also take on a level of importance that might not otherwise exist as the detection of adverse events could become a national security issue.

While it may be argued that this in fact only requires two architectures, and that the data warehouse type of structures used by researchers and the FDA could be used by the CDC, data sent to data warehouses is typically not sent in real-time, and is not patient identifiable. The creation of a data warehouse that could be used by all entities could potentially drive architecture for a data warehouse that was far more complex and robust than would typically be architected. This, in turn, would increase cost.

Realistically, any large-scale organization designs systems to manage large numbers of users (such as physicians and nurses) without an adverse impact to the overall performance of the system, while simultaneously ensuring that these systems do not have large amounts of unused capacity, i.e., we design systems to meet our needs while limiting overhead. Large organizations go through continuous and ongoing capacity-planning exercises to ensure that their networks and systems are sufficient for their needs.

In addition, most large corporations also have a need to analyze large amounts of data to manage their business more effectively, and to better understand how they are able to meet the needs of their clients. This is typically done through the use of data warehouses, data marts, and operational data bases. Information is extracted from core transaction systems (such as clinical, accounting and procurement systems) and placed in large data stores for analysis. Due to the nature of the analysis performed by large organizations, they typically do not allow for ad hoc reporting, research, and direct extraction of large amounts of data from an operational system during 'normal' business hours. If an organization has designed a system to be able to manage a certain number of transactions per day, any additional load, be it extraction of large data sets for research, or additional numbers of external users, can hurt the efficiency and viability of the system.

The impact of implementing various solutions needs to be evaluated, and we would suggest the following factors be considered:

- The creation of a minimum of two or possibly three separate architectures would result in higher implementation, capital acquisition and ongoing operational costs.

- Unless the creation of clinical data warehouses is done at the same locations as the RHIOs, additional support staff and expertise would be required for the ongoing support and maintenance of the structures.

- Vendors, in modifying their applications to meet the needs of the NHIN, could potentially be driven to meet the needs of differing requirements, which could, in turn, drive up the costs to vendors and result in conflicting requirements.

- Healthcare providers could be placed in a situation of having to modify existing legacy systems and processes to meet the needs of multiple solutions. The costs to providers of modifying systems are still a fairly un-quantified factor. This will almost certainly involve considerable expense on the part of any large organization needing to be a part of a RHIO, multiple RHIOs, or the NHIN, particularly in terms of how the RHIO or NHIN may query their systems.

If the needs of researchers and the CDC do in fact drive different solutions to those of the clinicians and patients, the implementation of different solutions could be considered as completely separate projects. As an example, the adoption of EHRs and the creation of clinical and patient portals may be set as the first objective for the NHIN, to be followed later by clinical data warehouses.

Similarly, different solutions could be implemented in parallel, but structurally and organizationally be treated as separate projects. While obviously requiring a great deal of cooperation, this could potentially allow for the different solutions to be treated and funded separately.

Simplicity: Key to Implementation and Adoption

Until now, the NHIN has been mostly discussed in high-level terms with only macro-level requirements being clearly articulated. We would suggest defining the micro-level of requirements. Certain key points seem to rise to the surface in talking about the NHIN and RHIOs, and these include cost, architecture, feasibility and ongoing support. In a typical infrastructure project, the aims of the NHIN are driven by the implementation of substantial IT infrastructures, and functional and non-functional requirements are key factors in determining costs. Non-functional requirements, such as response time and system availability needs, in particular are key factors in determining IT architecture.

While we realize and endorse the need for an informed and rigorous debate on the goals and implementation of the NHIN, we would encourage everyone to remain aware that as the functional and non-functional requirements for the NHIN are articulated, both the feasibility and cost of any proposed solutions will need to be revisited and validated as there may be changes.

Key benefits to providers from a focus on simplicity of design would include maximizing reuse of existing infrastructure and reduction in the degree of modification that legacy systems would undergo. The derived reductions in costs and implementation risk should broaden provider participation.

There are significant details in the areas of requirements and architectural decisions that should be addressed. These yet-to-be defined details will determine the level of solution complexity. Time-to-market, implementation costs and the degree of voluntary adoption may be hurt as complexity increases. ONCHIT has the opportunity to deliver a more adoptable solution earlier by keeping the solution focused on absolutely essential functionality, i.e., target simplicity as a design objective.

From the perspective of providers, some of the options that stand out as being the most costly and difficult to implement include:

- Patient Opt-In/Opt-Out
- Data Retention

Each of these is discussed below. It should be noted that similar issues and costs would be incurred in other areas, e.g., inclusion of digital images.

Patient Opt-In/Opt-Out

The capability for a patient to choose whether or not to make their data available to or accessible via NHIN for non-bioterrorism analytical purposes is certainly laudable from a privacy perspective. However, it should be noted that this feature could have significant impact on provider IT systems and business processes and may impact patient care.

If the Opt-Out capability is at an individual encounter level then:

- A new field would be need to be added to each of the clinical records for that encounter requiring additional disk space, software modifications, software testing, database administration and systems documentation changes.
- Additional fields(s) would also need to be added to each clinical registration system requiring software modifications, software retesting and registration documentation updates.
- Paper forms may require redesign.
- Registration personnel would require retraining.
- Audit processes would need to be adapted to monitor compliance.

A provider would incur cost, implementation risk and legal implications in implementing this type of capability. Providers will assess these factors against the benefits of participating in the NHIN.

Data Retention

Any increase in data retention requirements would represent a major cost factor for providers. For example, to meet the current legal requirements for data retention one leading provider has over 70 terabytes of text-based information in its primary clinical systems. For the same provider, Picture Archiving and Communication System (PACS) image storage is anticipated to grow to over 7 pedabytes over the next five years. In aggregate these storage devices, which were sized to accommodate current legal needs, represent an investment of over $100 million.

Beyond the quantity and size of the individual clinical records, the most significant factors determining cost for data storage are the length of retention and the speed of access. In the event of a regulatory change increasing the legal retention period, costs will rise linearly based upon the growth in the number of storage devices needed to store the data. Lower cost, albeit slower, secondary or tertiary storage devices (e.g., tape silos) could be leveraged for older data provided that the retrieval response times would be met.

The frequently stated objective of maintaining an individual's medical history for a lifetime has some applicability from a clinical perspective but may not be justified when viewed from a cost/benefit perspective. The storage and maintenance of such an increase in data volumes would bear significant costs. New mechanisms would need to be engineered to notify providers of mortalities so as to trigger data purge or archival processes.

Smart Card identification and storage devices would provide limited utility with the NHIN. Unfortunately there has been some public hyperbole setting an expectation that the technology can not deliver. At this point in time the technology supports approximately 1 kilobyte of volatile memory or 16 kilobytes of read only memory. These capacities would be inadequate for persistence of medical information. However, this technology would be excellent for identification purposes such as physician credentialing or storage of personalized encryption keys. Another potential usage of Smart Cards would be to expedite patient registration.

Incentive for Regulatory Simplification

There is a variety of clinical data reporting regulations, many of these being local public health reporting requirements. Some of these require patient identification (such as for infectious diseases), while others are reported de-identified (such as for near-miss medication errors). Reporting is currently done in a variety of formats, and through various reporting channels.

The NHIN has the potential to be a secure and standardized method for transmitting clinical information. This presents an opportunity to standardize regulatory reporting to a

single mechanism that all reporting could migrate to, with the associated cost savings. ONCHIT may also wish to explore potential of reuse of any data stores created for the NHIN or RHIOs as a source for regulatory reporting, in turn eliminating unnecessary data stores and their associated costs.

Regulatory reporting should be reviewed to eliminate alternate methods and reduce the costs to support multiple reporting methods.

HIPAA

A considerable amount has already been written and discussed on the issues surrounding privacy and the RHIO and NHIN. However, the objectives of HIPAA and an NHIN must be balanced to enable adoption of an NHIN. Particular areas we would like to spotlight are:

- There will need to be clarity regarding accountability once data leaves a single entity. As an example, a large provider might have extremely tight security around their internal systems, but send patient data (identifiable or de-identified) to a RHIO or data warehouse. In the event of a breach of security in the case of a centralized data model, the accountability of all parties involved would need to be clear. Lack of clarity in this area may result in a reluctance to adopt the technologies.
- In light of the large number of Internet fraud, aka 'phishing,' attacks seen lately on the Internet, clarity would be advisable in the event of a patient compromising the security of their own PHR due to being misled by phishing.
- The legal status of new entities created by the implementation RHIOs or the NHIN would need to be clarified under HIPAA as these entities do not appear to meet the definition of a HIPAA covered entity (45 CFR §160.103). Furthermore, it is unlikely a RHIO or NHII would meet the definition of a business associate (45 CFR §160.103) nor would a provider want the liability of designating them as one.
- The potential use of patient matching algorithms to combine data in a RHIO could provide a unique situation in a patient portal. Should incorrectly matched data be displayed in a single record, a patient could potentially have access to another patient's record, not through a breach of security but through failure of the technology.
- Providers must determine how the minimum necessary standard (45 CFR §164.502) may be met with allowing access or obtaining access to protected health information through a RHIO or NHII.
- HIPAA's Standards for Privacy of Individually Identifiable Health Information (45 CFR 160 and 164) elevated patients' providers, insures, governmental agencies sensitivity of protected health information. Healthcare providers store tremendous amounts of health information. As custodians of health information, providers are ethically and legally held accountable for the integrity and

confidentiality of the information. We question how providers can determine if a RHIO and or NHIN can be entrusted with the patient's information. Providers would face a substantial burden if required to individually evaluate a RHIOs technological solution, security and operations. For widespread adoption of a NHIN, RHIO certification would need to be driven by HHS.

- Mandatory or voluntary submission of patient identifiable health information to the RHIO or NHIN would be a burden on a facility as these disclosures would likely be required for inclusion in the accounting of disclosures (45 CFR §164.528). Other accounting of disclosure burdens could arise from RHIO or NHIN security breaches.
- Consideration must be given to how the RHIO or NHIN would operationalize a provider denying a patient access to their PHI (45 CFR § 164.524), granting a patient's request for a restriction (45 CFR § 164.522), and granting a patient's request for amending their record (45 CFR § 164.526).

Need for National Standards

Interoperability in information technology that isn't standards-based is possible, but tends to be cost prohibitive to implement and difficult to maintain. Definition and governance of standards at a national level would reduce the complexity and risks of implementation allowing for wider and more consistent adoption. A minimum set of standards would need to address interoperability, interfacing (including web services), communications, security, and base application services. Standards must address the NHIN at all levels, particularly the RHIOs. Standard definitions need not include directives on specific infrastructure, commercially available software, or tooling.

We suggest that ONCHIT:

- Mandate existing bodies, such as *HL7, ASTM and SNOMED,* to set standards, while outlining the framework for defining standards.
- Encourage the adoption of existing standards and technologies where feasible
- Set standards for vocabulary, electronic health record components and messaging.
- Document the above standards via a publicly accessible website.
- Put in place a federal standards commission with responsibility for reviewing the standards on a yearly basis, and for approving new standards adoptions by accredited bodies prior to adoption.
- Discourage the adoption of differing standards levels that would inhibit interoperability among RHIOs.
- Encourage public/private certification entities based on adopted standards.

Financial Impact on Providers

Participation in the NHIN will require a significant investment in financial and human resources by providers with substantial existing HIT systems. Many of these systems were developed and implemented without consideration of participation in a larger national information exchange and infrastructure. Many of these systems have been purchased from software vendors thus adding to the complexity of making changes. As a result, modifying these systems and our associated business and clinical processes will place an increased cost and administrative burden on healthcare providers. It should be

noted that there are no quantified cost offsets for providers implementing access to the NHIN. As mentioned earlier in this document, providers will need to weigh the expected clinical benefits derived from involvement against the financial considerations.

Preliminary quantification of the impact will not be possible until specific requirements are established and some key architectural decisions begin to gel, e.g. peer-to-peer versus centralized repository. While it would be premature to assign a dollar estimate to the effort, some general categories of costs can be identified.

Duplicate Source Systems

Access by the public, other healthcare entities or government agencies to the internal data stores of organizations' existing systems would provide significant challenges in the areas of security and performance management. The security issues such as unauthorized access, hacking and virus attacks are documented elsewhere within this document. All legacy systems are sized for performance and capacity based upon the anticipated needs of their organization. No accommodation will typically have been made for resource burdens originating from external entities. For example, if an external resource executed a long running query against a clinical system, the response times to that provider's hospitals could adversely impact clinical activities, which would clearly not be acceptable. Duplicate or augmented infrastructure would be necessary to address this situation.

Security Infrastructure

Connection to the NHIN will require careful consideration of opportunities for malicious attack against legacy systems and unauthorized access to privileged data. These concerns are not unknown to providers that have Internet or other public access to their systems. However, the NHIN may require some providers to implement such public access for the first time and also require providers to allow access deeper into their corporate IT systems.

Security appliances such as firewalls, intrusion detection and reverse proxies will be necessary to support access to legacy applications.

Authentication and authorization repositories and mechanisms will need to be established and maintained.

Augmented solutions for virus detection, network and resource monitoring, activity logging and log analysis will need to be implemented.

Communications Infrastructure

Enhanced access to the Internet or to a private network, such as that provided by the Internet 2 project for research and higher education, will be required to support many of the proposed services of the NHIN. Significant incremental bandwidth may be necessary based upon the final requirements and response time objectives. Also significant, additional bandwidth may be necessary should PACS or other high impact image traffic be included within the NHIN.

Storage

As stated in the section entitled 'Duplicate Source Systems,' mirror, or replicated versions of the production disk space may be required if the NHIN is implemented as a peer-to-peer topology.

Incremental disk space may also be necessary should the period of data retention be increased. Usage of cheaper bulk archival or other secondary or tertiary storage may be leveraged, assuming that the request response time objectives could be met.

Additional disk space will be necessary to support any data elements added in support of the NHIN. An example might be the addition of an Opt-In/Opt-Out flag on clinical records.

Modifications to Legacy Applications

Most clinical systems will require either modification or upgrade. Significant resources may need to be extended in the analysis of the changes, implementation, testing and/or certification of these solutions.

Upgrades of operating systems, database products or other system tools may be necessary to support these enhancements.

Software

New software products or development will be necessary to support the NHIN. These products or development efforts would include web services, application services, Enterprise Application Integration (EAI), Extraction-Transformation-Loading (ETL), security tooling, database management systems, data analysis and reporting tooling.

Operational Processes and Procedures

The changes to existing system operations may be profound based upon the requirements of NHIN. New jobs may need to be integrated into already tight batch windows to implement functions such as data extraction. New monitoring of servers and interfaces will also need to be implemented.

Help Desk processes will need to be extended to support both the operational needs of the NHIN as well as the capability to support clinical end-users.

Clinical Processes

Changes will need to be made to the admissions process and automated systems to accommodate acquisition of any additional information required for the NHIN.

Clinical users of the NHIN will need to be trained on the capabilities and "how to" procedures.

Training

The NHIN will require development of training materials and delivery of some degree of training within many areas of the provider organization. Personnel who would be most clearly impacted are registrars, clinicians, health information management, operational systems support, help desk and security resources.

Technical Feasibility of Key Functionality

It needs to be noted that considerations of cost versus function are not always absolute givens. There is often a belief when dealing with technology-based implementations that the only question is if we are prepared to pay enough to meet a given requirement anything is achievable. It needs to be noted that even with all the advances in information technology in the last quarter century, there are still barriers which make the implementation of certain IT systems unfeasible due to technical and physical rather than financial constraints.

The following sections cover areas of key functionality which we are of the opinion will require special consideration in architecting and implementing a viable solution.

Matching patient information

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

In some cases the social security number has become a de facto mechanism for matching patient data in health systems, however even that presents issues. As with other systems, the larger the system becomes the greater the risk of making errors in the matching of patient data. What may be a viable solution for a chain of 3 hospitals may not scale to a RHIO of 15 facilities, and what works for a smaller RHIO may not scale to a larger RHIO. The requirement to retrieve an individual patient record at a national level has not been fully articulated, but should that become a requirement the problems associated with matching of patient data will be that much greater.

In this regard there is no clear requirement as to what level of error would be acceptable in matching patient records, and whether the incorrect matching of records could be considered a risk to an individual patient.

As solutions are proposed for the matching of patient records both regionally and nationally, we would again make a call for simplicity of design, and the creation of solutions that are scaleable from a regional to a national level.

Storage of Patient Information, Retention of Data and Bandwidth

Over and above the potential issues already discussed regarding the cost of retaining large amounts of patient data in central locations, we would like to put forward the following considerations.

Most large organizations spend considerable time and effort in creating, adopting and managing policies around retention of data. Retention of data is a constant juggling act between retaining data that is necessary (from an operational or legal perspective), and the impact of retaining too much data. Some presentations on the NHII have dealt with the concept of maintaining patient data for the lifetime of the patient. There is a tendency

to treat this topic as a technical and cost discussion, but a number of factors, many of which are not as obvious at first glance, play a role in this discussion:

- Data requires storage, storage requires hardware. We have already dealt with some of the implications of storing large volumes of PACS images, but even the centralized storage of large volumes of textual information in a country the size of the United States presents significant cost challenges.
- Data should be useful and relevant. While it is true that some data is stored for legal purposes, it is equally true that not all clinical data remains relevant for the lifetime of the patient. For example, a negative x-ray of a 40 year old patient showing they did not have pneumonia at age 26 may be of little relevance at age 40.
- Too much data can be as much of an issue as too little data. At the July 2004 NHII summit this issue was raised on more than one occasion. For information to be useful not only must it be relevant, but it must be easily accessible to the clinician.
- Too much data can impact performance. Data is stored in databases which are indexed to allow retrieval of data in a timely manner. Retrieving a single record from a database of 10,000 records will, by its nature, be far quicker than retrieving the same record from a database of 1,000,000. While the storage of all relevant patient detail is clearly a valid and desirable objective, the associated system performance characteristics need to be taken into consideration.
- In a decentralized model data must be retrieved from source systems. The more data is stored, the more information in terms of bytes will need to be retrieved. This has an impact on bandwidth, data retrieval times and latency. All of these factors in turn could potentially drive up cost.

We would suggest ONCHIT consider proposing the setting of standards for data retention at a central level. Issues around data-retention may not be as great an issue when RHIOs and the NHIN are first implemented. However, if data is retro-actively included in the NHIN (as has been discussed in the NHII proposals), the amounts of data stored and the ability to retrieve the data could rapidly become an issue.

Availability and Redundancy

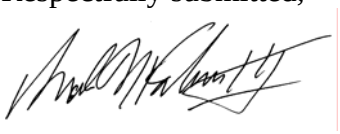
Availability and redundancy of data are both non-functional requirements and operational characteristics. Both are factors in architecture and cost, as well as technical feasibility. In considering the technical feasibility of the implementation of RHIOs and the NHIN, we feel the following factors need to be considered:

- Availability of any given system is dependent on factors such as bandwidth, scaling, throughput and latency. Wise choices need to be made with regard to the types and quantity of data required to meet the needs of the NHIN with regard to patient care, patient portals and research.

- If the patient care portal is to become the primary point of care for clinicians, the ability of the portal to provide information in a timely and complete manner will in turn affect the quality of patient care. Particular care needs to be taken when choosing architecture to ensure it can scale from small to large scale operations, can handle the volumes of data as the systems increase in size, and they can handle volumes of data without a drop in response time.
- If systems are to be used as a point of primary care, they need to be designed in such a way that they are fault-tolerant and redundant throughout. This includes the network layers, server architecture, and communication channels. The feasibility of the Internet as a medium for transferring large volumes of data needs to be validated if it is to be used for these purposes.
- The network requirements for transferring large sets of data at regular intervals (as may be required for use by the FDA, CDC and research bodies) need to be evaluated and architected accordingly.
- The impact of downtime to all users (clinician, patient, researcher etc.) needs to be evaluated, and relevant architecture put in place based on requirements.

On behalf of our members, FAH appreciates this opportunity to comment on this important request for information. As stated above, FAH strongly supports the aims of the NHII. We recognize the complexity of the issues and commend HHS for its willingness to thoughtfully engage and work cooperatively to balance competing concerns on many different topics. We look forward to ongoing efforts to achieve our collective goals.

Respectfully submitted,



Charles N. Kahn III
President

Appendix: 4

APPENDIX 1 – CROSS-REFERENCE OF RFI QUESTIONS AND RESPONSES

Question 1

The primary impetus for considering a NHIN is to achieve interoperability of health information technologies used in the mainstream delivery of health care in America. Please provide your working definition of a NHIN as completely as possible, particularly as it pertains to the information contained in or used by electronic health records. Please include key barriers to this interoperability that exist or are envisioned, and key enablers that exist or are envisioned. This description will allow reviewers of your submission to better interpret your responses to subsequent questions in this RFI regarding interoperability.

Page 1 Paragraphs 2 & 3
Page 2-4
Page 4 (Simplicity: Key to Implementation and Adoption)
Page 6 (HIPAA)
Page 7 (The Need for National Standards)
Page 8 (Financial Impact on Providers), Page 10 (Technical Feasibility of Key Functionality)

Question 2

What type of model could be needed to have a NHIN that: allows widely available access to information as it is produced and used across the health care continuum; enables interoperability and clinical health information exchange broadly across most/all HIT solutions; protects patients' individually-identifiable health information; and allows vendors and other technology partners to be able to use the NHIN in the pursuit of their business objectives? Please include considerations such as roles of various private- and public- sector entities in your response.

Pages 2-4
Page 4 (Simplicity: Key to Implementation and Adoption)
Page 7 (Need for National Standards),

Question 3

What aspects of a NHIN could be national in scope (i.e., centralized commonality or controlled at the national level), versus those that are local or regional in scope (i.e., decentralized commonality or controlled at the regional level)? Please describe the roles of entities at those levels. (Note: "national" and "regional" are not meant to imply federal or local governments in this context.)

Pages 2-4
Page 7 (Need for National Standards)
Page 10 (Matching Patient Information)

Question 4

What type of framework could be needed to develop, set policies and standards for, operate, and adopt a NHIN? Please describe the kinds of entities and stakeholders that could compose the framework and address the following components:

a) How could a NHIN be developed? What could be key considerations in constructing a NHIN? What could be a feasible model for accomplishing its construction?
Page 2-3
Page 4 (Simplicity: Key to Implementation and Adoption)
Page 8 (Financial Impact on Providers)
Page 10 (Technical Feasibility of Key Functionality)

b) How could policies and standards be set for the development, use and operation of a NHIN?
Page 7 (Need for National Standards)
c) How could the adoption and use of the NHIN be accelerated for the mainstream delivery of care?
Page 7 (Need for National Standards)
d) How could the NHIN be operated? What are key considerations in operating a NHIN?

Question 5
What kind of financial model could be required to build a NHIN? Please describe potential sources of initial funding, relative levels of contribution among sources and the implications of various funding models.
Page 7 (Financial Impact on Providers)

Question 6
What kind of financial model could be required to operate and sustain a functioning NHIN? Please describe the implications of various financing models.
Page 8 (Financial Impact on Providers)

Question 7
What privacy and security considerations, including compliance with relevant rules of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), are implicated by the NHIN, and how could they be addressed?
Page 6 (HIPAA)
Page 9 (Security Infrastructure)

Question 8
How could the framework for a NHIN address public policy objectives for broad participation, responsiveness, open and non-proprietary interoperable infrastructure?
Page 4 (Simplicity : The Key to Adoption)
Page 7 (The Need for National Standards)

Question 9
How could private sector competition be appropriately addressed and/or encouraged in the construction and implementation of a NHIN?
Page 7 (The Need for National Standards)

Question 10
How could the NHIN be established to maintain a health information infrastructure that:

a) evolves appropriately from private investment;
b) is non-proprietary and available in the public domain;
c) achieves country-wide interoperability;
d) fosters market innovation.
(Page 7 (The Need for National Standards)

Question 14
What kinds of entity or entities could be needed to develop and diffuse interoperability standards and policies? What could be the characteristics of these entities? Do they exist today?
Page 7 (The Need for National Standards),

Question 15
How should the development and diffusion of technically sound, fully informed interoperability standards and policies be established and managed for a NHIN, initially and on an ongoing basis, that effectively address privacy and security issues and fully comply with HIPAA? How can these standards be protected from proprietary bias so that no vendors or organizations have undue influence or advantage? Examples of such standards and policies include: secure connectivity, mobile authentication, patient identification management and information exchange.
Page 7 (The Need for National Standards),

Question 16
How could the efforts to develop and diffuse interoperability standards and policy relate to existing Standards Development Organizations (SDOs) to ensure maximum coordination and participation?
Page 7 (The Need for National Standards),

Question 18
What roles and relationships should the federal government take in relation to how interoperability standards and policies are developed, and what roles and relationships should it refrain from taking?
Page 7 (The Need for National Standards),

Question 20
What kind of incentives should be available to regional stakeholders (e.g., health care providers, physicians, employers that purchase health insurance, payers) to use a health information exchange architecture based on a NHIN?
Page 8 (Financial Impact on Providers)

Question 21
Are there statutory or regulatory requirements or prohibitions that might be perceived as barriers to the formation and operation of a NHIN, or to support it with critical functions?
Page 6 (HIPAA)

Question 23
Describe the major design principles/elements of a potential technical architecture for a NHIN. This description should be suitable for public discussion.
Pages 2-4
Pages 10-12