Department of Health & Human Services

Office of the National Coordinator for Health Information Technology

Federal Health Architecture
Review of Nationwide Health Information Network (NHIN)
Functional Requirements

Version 4.0

July 27, 2006

**Office of the National Coordinator for Health Information Technology
Washington D.C.**

Table of Contents

List of Tables

1.   Introduction

At the request of the Office of the National Coordinator for Health Information Technology (ONC), the Federal Health Architecture (FHA) Program Office undertook an effort to coordinate federal participation in the review of functional requirements for the Nationwide Health Information Network (NHIN). Through a series of collaborative sessions and the efforts of five federal role-based teams, the FHA produced a (1) summary set of comments and (2) analysis documented in Excel spreadsheet format and included as Appendix A.

1.1   Document Purpose

This document is intended to provide the National Committee for Vital Health Statistics (NCVHS) with a summary assessment of the existing NHIN functional requirements from the federal agency perspective.

1.2   Scope

The focus of the review was on assessing 1) whether the existing functional requirements are 'minimal and essential'; 2) whether the requirements meet the needs of the federal agencies (referred to as "Federal Fit"), and 3) what minimal but essential requirements are missing.

The following items are considered out-of-scope for purposes of this review:

- Requirements that fall into the five (5) non-functional requirement categories: robustness, performance, accuracy, business rules and scalability
- Policy related requirements.

1.3   Methodology Used

The methodology used to conduct this review is summarized below:

- The FHA Program received the NHIN requirements June 12th, 2006. The requirements consisted of 977 statements enumerated in Appendix A.
- FHA led five review teams, organized according to agreed upon roles (1) Consumer, (2) Payer/Administrator/Regulator, (3) Provider, (4) Researcher/Educator, (5) Surveyor, to comment on these requirements. The teams consisted of members from twenty federal agencies. A kick-off meeting was held May 23, 2006. General collaboration sessions were held weekly through June 27, 2006. Role Team meetings were held two or more times a week from June 13th through June 26th 2006.
- The comments (summary and detailed) were used by federal agency representatives as a reference during their participation in the ONC sponsored Forum on NHIN Functional Requirements held June 28-29, 2006.
- A follow-on team of subject matter experts (SMEs) used the results of this review in the second stage of analysis. The follow-on team's approach is summarized below:
    1. Team members were assigned functional categories based on the reviewer's area of expertise. Each team member independently reviewed and analyzed the requirements

within their assigned functional category based on expert judgment, the number of role-based teams that indicated that the functional requirement was a critical need, and comments provided by the role-based assessment groups.

2. Given the timeframe available for the review, the team narrowed the review of the requirements to answer the following 3 questions:

- Is the functional requirement essential to the system? (The evaluation criteria included the results of the role-based review conducted by federal agency representatives.)

- Does the functional requirement meet the federal agencies' needs?

- If needs are not met, what gaps remain to be addressed?

3. Results of each member's analysis were then combined and aggregated. See Appendix B for mapping of the 6 aggregated categories to the 20 functional categories as defined in Nationwide Health Information Network Functional Requirements; April 16, 2006.

1.4   Document Organization

This document is organized as indicated in Table 1 below.

Table 1: Document Organization

Section		Purpose
Section 2:	Initial Observations	Identifies the initial observations for the Functional Requirement Review.
Section 3:	Review of Core Functional Requirements	Presents the results of functional requirements analysis
Section 4:	NHIN Standards Review	Presents the results of our review of standards relevant to NHIN and each use case
Section 5:	Next Steps	Provides recommended next steps for NCVHS
Appendix A:	Nationwide Health Information Network Functional Requirements	NHIN Functional Requirements
Appendix B:	NHIN Mapping of 20 Functional Categories to 6 Aggregate Categories	Summary presentation of the Functional Categories.
Acronym List		Defines the acronyms used in this document.
List of References		Provides a list of the references used in the preparation of this document.

2.   Initial Observations

1. The existing functional requirements form a useful basis for a "minimum and essential" set. The great majority of the existing functional requirements should be retained and included in the initial set.

2. It is understood that the existing functional requirements were developed primarily around the American Health Information Community (AHIC) Breakthrough Use Cases so it is expected that additional functional requirements will be needed to produce a set of functional requirements that meet the remaining needs of the federal government. The gap between the existing set and the desired set is enumerated below.

3. The existing requirements were structured around 20 functional categories. It would be useful to systemically map the existing requirements to the business-oriented role based framework used in the FHA review. This could be done at the category level or at an individual requirement level to ensure completeness, ensure consistency, make the requirements more readable and understandable, and establish clearer interrelationships between requirements.

4. The existing functional requirements address well the "as is" state of interoperability. It will be useful at some point in the development to develop a set of requirements that include a vision, concept of operations and business processes based on a future or "to be" state of interoperability.

5. A clear definition of the content, syntax, and semantics for the functional requirements was published in the guidance to the authors of the existing functional requirements; however a number of the existing functional requirements still need to be refined to address specific business behaviors that will be satisfied by the NHIN. Existing requirements include some design-oriented language including system characteristics, system-oriented business rules and overly granular descriptions approaching design specification. Some requirements need to be reworded to be clearly neutral on policy issues.

6. It is understood that NHIN will conform to existing legislation including security related needs and the implications of supporting the Federal Information Security Management Act (FISMA) and other government legislation (e.g., NIST 800-53, HSPD). It would be useful to develop a document mapping functional requirements to existing standards and legislation to compliment the functional requirements.

3.   Review of Functional Requirements

The scope of this review is 896 of the original 977 functional requirements. This review did not include the 86 non-functional requirements, as shown in table 2 below.

Table 2: Functional Requirements Reviewed

Aggregate Functional Categories	Reviewed	Not Reviewed
Data Content	191	-
Data Storage	32	-
Data Transaction	327	-
Data Transformation	87	-
Information Location	81	-
Security	178	-
Non-Functional	-	91
Total	896 (91%)	91 (9%)

This section summarizes the results of the follow-on assessment of the 896 remaining functional requirements.

3.1   Summary of Results by Aggregate Functional Categories

Table 3 below summarizes the results of our analysis.   The vast majority of existing requirements are considered essential, as well as critical from the perspective of the federal agencies ("federal fit"), but they are not complete -- some gaps exist that must be addressed to fully address federal needs. Section 3.2 below summarizes what is essential within each of the 20 functional categories. Section 3.3 highlights the gaps.

Table 3: Summary of Results

	Aggregate Category	# FRs	% Federal Fit	% Essential "Core"[1]	% Essential "Edge"[2]	Gaps
1	Data Content	191	190 (99%)	30 (94%)	154 (97%)	Yes
2	Data Storage	32	31 (97%)	4 (100%)	27 (100%)	Yes
3	Data Transaction	327	326 (100%)	101 (94%)	200 (92%)	Yes
4	Data Transformation	87	85 (98%)	15 (88%)	62 (91%)	Yes

---

[1] Based on the subset of requirements considered to be a "federal fit."   That is, the requirements considered to be essential were those already considered to be a federal fit.

[2] Based on the subset of requirements considered to be a "federal fit."   That is, the requirements considered to be essential were those already considered to be a federal fit.

5	Information Location	81	80 (99%)	56 (98%)	22 (96%)	Yes
6	Security	178	168 (98%)	67 (96%)	86 (91%)	Yes
	TOTAL	896	880 (98%)	273 (95%)	538 (94%)	

Ninety-eight percent (98%) of the 896 requirements reviewed were considered to be a "Federal Fit" (i.e., were considered necessary requirements from the perspective of the federal agencies). The remaining requirements had little to no impact on meeting federal needs as these requirements were either not necessary to meet federal regulations, were covered by another functional requirement, or could be phased in at a future time.

Of the 880 remaining 'good Federal Fit' requirements, the team identified those that met the criteria for 'minimal and essential' in each of the 6 aggregate categories across "core" and "edge" systems. Ninety-five percent of the remaining 'core' requirements are considered 'minimal and essential' and 94% of the remaining 'edge' requirements are considered 'minimal and essential.' See Section 3.2 for a summary of this assessment.

It is important to note that based on Version 3 of the NHIN Proposed Functional Requirements guideline dated April 16th, 2006[3], many of the minimal and essential requirements identified fall outside of the definition of functional requirements (business-oriented interactions, services or functions). They are often policy/legislation or design-oriented requirements. It is possible then that the overall number of NHIN well-articulated functional could be reduced.

3.2   Assessment of "Minimal and Essential"

The first question this analysis intended to answer was, "To what extent are the existing NHIN functional requirements considered 'minimal and essential' for federal agencies?" The team assessed a requirement as "minimum and essential" if it was considered a necessary business function that the system must satisfy and it is needed in even the most "stripped down" version of NHIN that is acceptable to the federal health community (based on their participation in the FHA collaborations).

---

[3] NHIN Proposed Functional requirements v3, April 16, 2006 – Overview – In general, functional requirements designate specific "properties" (functions, services, behaviors, and technical and processing needs and capabilities) of "entities" (systems, services, networks and, at times, actors).

Table 4 below highlights the essential functional requirements in each of the 20 functional categories.

Table 4: Summary of Results -- "Minimum and Essential" Analysis

	Category	Summary-Level Essential Functional Requirements
1	Audit and logging	• Functionality to support auditing and logging, supporting the capability to assess systems for nefarious activities, detect reportable activities, ensure confidentiality and integrity of patient and other sensitive data, investigate and resolve security breaches in a timely manner, and manage guidelines across multiple federal regulations (SOX, HIPAA, FISMA, etc.) • Capability to generate alert notifications – generating alerts/notifications for activity outside the normal range of monitoring levels. Supports bio-surveillance and anti-terrorist activities (HSPD 7 Critical Infrastructure Protection) • Ability to generate evidence to support incident management and response processes (e.g. virus /worm attack or denial of service, evidence must be captured) provides a high-level security posture • Functional requirement for an easy to use interface to message history logs and support rebuilding of patient medical records at specific points in time
2	Authentication	• Functional requirement for a secure robust user authentication system to support multiple authentication mechanisms including but not limited to username/password, X509 or other standard certificate and smart card. • Capability to permit single session authentication that allows user access to different applications within the NHIN • Provide a mechanism for ensuring non-repudiation for output that requires verification • Accept first time log-in identification data from consumer (this will generate broader acceptance and higher usability rates among consumers and patients)
3	Authorization	• Consent Management. The NHIN system must be flexible and capable of handling multiple consent states (implied consent/dissent, expressed consent/dissent, undetermined). • Provide capability to implement a data restriction service. It must be possible for a user to restrict access to a specific data set related to a medical diagnosis/treatment based on his/her professional discretion, on the request of the individual, legal requirement, or other legitimate reasons. • Functionality to support role-based access (RBAC). RBAC model must be able to support large scale user expansion and varying types of access privileges. RBAC is necessary to assign and manage access privileges for all NHIN users and interfacing Edge Systems.

	Category	Summary-Level Essential Functional Requirements
4	Confidentiality	• System Monitoring Functionality. A robust monitoring capability is required to ensure that security controls are operational, are effective, and are observed by all staff and third parties (where appropriate). • Encryption Capability. Protect confidentiality and integrity of data and services over the network using encryption. • Upon request, capability to provide patients with a list of institutions or providers requesting information about them. (HIPAA requirement) • Ability to attach randomized linker before transmission of patient specific data that supports ability to re-identify data when required as part of an authorized public health investigation • Functionality to anonymize data for transmission to public health agencies • Capability to support transport level security • Capability to implement a randomized data linker (RDL) for biosurveillance data transmitted to public health agencies (HSPD 7 Critical Infrastructure Protection)
5	Credentialing	• Capability to register user and administrator community including but not limited physician, patients, consumers, edge systems and public health administrators.
6	Data access and update	• Functionality that provides a secure electronic patient demographic and health history which can be accessed, viewed and updated by the consumer and shared with others at the consumer's choice • Functionality that allows payers, providers, patients and other stakeholders the ability to share information to support medical research, drug safety, and post-marketing drug surveillance. • Capability to accept inserts, updates and deletes to payers, providers, patients, and other stakeholders' data.
7	Data content	• Capability to transmit well formed messages according to a HITSP specified implementation instruction. • Capability to conform to approved, vocabulary, structure, privacy, security and messaging standards as provided by HITSP when transmitting patient data
8	Data filtering	• Provide capability for clinician to request all available data (from local and remote communities) for specified patient • Provide clinician capability to query for results based on one or multiple criteria for a specified patient • Functionality to support various filters for queried or returned data, including filtering on a specific order number (e.g. accept a filter rule defined by public health agencies)
9	Data mapping/ translation	• Capability to transform data using approved standards as provided by HITSP or as agreed upon with ONC content and messaging standards • Ability to offer 'translation' services to provide clinical data in easy to read and understandable format and language • Functionality to support translating data into appropriate standards for incorporating data into EHRs
10	Data quality/data integrity	• Ability to use integrity verification information to validate the integrity of data received across the network • Capability to verify integrity of unsolicited result transactions • Functionality to send error message to remote marketplace if not authenticated or if consent of data locations message is not verified

	Category	Summary-Level Essential Functional Requirements
11	Data rendering	• Functional requirement to provide patients with the capability to access to their personal health record (PHR) • Give providers the ability to access to view information on specific patients • Give providers the ability to view and order laboratory, radiology, or other medical image information
12	Data retrieval (pull)	• Functionality to transmit queries that are formatted according to HITSP standards and implementation guides for consumer health data to a PHR system. The query will contain the PHR location and patient/consumer provided credentials. • Capability to conform to approved, vocabulary, structure, privacy, security and messaging standards as provided by HITSP when transmitting patient data • Ability to aggregate query responses from multiple data sources and return a single aggregated response to the querying entity.
13	Data routing	• Functionality to accept and route all authorized messages to designated edge systems • Capability to determine the method of message delivery to the final destinations • Ability to determine entities to receive biosurveillance event response "broadcast" messages based on authorization by sender and subscription by receiver to support event response
14	Data source	• Capability to accept and apply various filters as part of an incoming query, for example results for a specific Lab order number. • Ability to identify source of externally-provided data
15	Data transmission (push)	• Functionality that allows the communication of approved PH updates and alerts to the public media via secure NHIN messaging to monitor a previously detected event • Ability to transmit aggregated anonymized data to public health systems in formats defined by the public health agencies. • Capability to conform to approved, vocabulary, structure, privacy, security and messaging standards as provided by HITSP when transmitting patient data.
16	Data usage	• Ability to communicate patient health data to other edge systems in the NHIN standard message format. • Functionality to generate aggregated anonymized data for federal public health agencies. • Generate alerts/notifications to public health users based on public health algorithms.
17	Identity/ information correlation	• Capability to determine unambiguous match of patient identities supported by entities associated with the network • Ability to minimize double counting. The system should be able to determine when multiple and or independently submitted data refer to the same case (patient) or event.
18	Persistent data storage	• Capability to store, maintain and have capability to retrieve data for amount of time required by law (Federal, state, local) • Capability to store multiple types of clinical data (Lab, Rx, diagnostic, procedure reports, genomic data, patient teaching, clinical progress notes, etc) • Capability to store all data using standard format and vocabulary
19	Record location	• Functionality to return pointers that enable retrieval of patient records from data sources / repositories • Functionality to notify requesting edge systems that identified edge systems contain the requested data.

	Category	Summary-Level Essential Functional Requirements
20	Transient data	• Capability to hold and aggregate data or error messages received from the data repository as determined by the community. If the data stager receives the data from the data source on behalf of the clinician, the data stager may: 1) hold and aggregate data from each data source and transmit to clinician when all queried data sources have responded to the request 2) hold data received until a time limit specified by the marketplace has been met, sending the remaining response as they are received 3) immediately send data as it is received from each data source of data from each queried data source.

An example of a functional requirement that was considered minimal but not essential for the first version of NHIN is described below. Federal input indicated that these kinds of requirements are very important but could be considered at a future phase of implementation, or when downstream design and cost implications could be resolved.

- Multiple-factor authentication for users (FHA568) - As stated in the federal comments: Multifactor authentication need not be considered a "minimum and essential" requirement. It is a best practice for ensuring that users of the system "are who they say they are"; however, it may not be a good fit for the initial phase release. Multifactor authentication will require outside entities to spend money for either a new technology or for use of an existing application. Moreover, security systems tend to require re-engineering or development work in order to mix and match technologies (i.e., RSA key fob and Netegrity SSO do not easily function together, likewise, many PKI solutions are not interoperable and these technologies are commonly used to support multifactor authentication).

3.3   Summary of Gap Analysis

The second question this analysis intended to answer was, "What functional requirements are missing to fully meet the need of federal agencies?" That is, what are the gaps?

Table 5 identifies the summary-level gaps from the federal perspective. Many of the gaps identified here are a result of the small set of use cases used to develop the functional requirements. The resulting functional requirements do not address the full functionality required meet federal business needs.

Table 5: Gaps in Functional Requirements by Category

	Category	Gaps in NHIN Functional Requirements
1	Audit and logging	• Functionality to address requirement for the disposal or destruction of audit data. • Functionality to address the retention periods for patient data • Capability to support the implications of legislative mandates on design and development of the NHIN (i.e.; FISMA, Privacy Act, etc.) • Ability to address throughput of system given auditing/logging requirements.

	Category	Gaps in NHIN Functional Requirements
2	Authentication	• Capability to generate authorization for re-linking identity information to anonymized data per RDL prior to re-linking the information. • Ability to expand to "all" the principal context of re-linking • Support the implementation of a secure mechanism for transmission of user credentials during authentication process.
3	Authorization	• Capability to fully support registration requirements (i.e. key components, approvers, authorizations, out-of –band registration, etc.) • Capability for individuals to authorize their consent to data usage/access. • Ability to permit access to an individual's data to Edge System users when authorized or where there is a legitimate need (as defined by law). • Ability to permit override of access restrictions to an individual's data by Edge System users (as defined by law). • Support the specific roles of research for access to patient and de-identification of data. • Capability for CDO's to opt-out of biosurveillance activities
4	Confidentiality	• Functionality to enable systems to securely transmit data outside of the health architecture and between entities within the health architecture. This requirement will have to be met in order for Federal entities to participate and to meet the requirements of HIPAA.
5	Credentialing	• Capability to register providers who participate in NHIN. This requirement will have to be more granularly refined to take into account the need for ensuring that credentialing information is accurate along with the NPI.
6	Data access and update	• Support the need for a consistent methodology for granting access (e.g., role or system interface) – need structured process to support existing and new workflows • Capability to provide a structured, approved emergency access process (in place of a general "Break the glass" requirement) • Capability to provide a structured, approved remote access process.
7	Data content	• No gaps identified.
8	Data filtering	• Functionality to support a hierarchical data structure with clarified metadata definitions to enable filtering • Capability to enable the process that governs filtering capabilities (e.g., who has ability to filter certain patient data), particularly regarding the legal and privacy implications of access and data aggregation • Capability to enable patients and clinicians to report adverse medical events and/or errors
9	Data mapping/ translation	• Support for specific standards or protocols required (e.g., HL7, SNOMEDCT, HIPAA) to allow data mapping and translation among disparate systems in an efficient manner • Capability to support Section 508 compliance (e.g., handicapped access, multiple language needs, etc.)
10	Data quality/data integrity	• Covered by non-functional requirements.
11	Data rendering	• Functionality to fully address and enable data collection and presentation capabilities mandated by federal standards (including HL7, SNOMEDCT, and HIPAA)
12	Data retrieval (pull)	• Capability to leverage a full data model and data dictionary (consistent metadata) as a basis for any kind of data retrieval

	Category	Gaps in NHIN Functional Requirements
13	Data routing	• Capability to support routing and alerts based on roles and organizational responsibilities (and not managed on a point-to-point basis) • Support for auditable data exchanges for messages requiring confirmed delivery or acknowledgement of (e.g., automated registry notification/information to and from chronic disease and other disease-specific registries for epidemiological studies and patient follow-up and monitoring) receipt. These are addressed by standards such as HL7, SNOMEDCT, and HIPAA.
14	Data source	• Suggestion to expand requirements to include a common data dictionary and metadata
15	Data transmission (push)	• Capability to ensure acknowledgment of accurate receipt from receiving core/edge system and/or retransmit if necessary • Functionality to provide real-time, bi-directional, standardized secure messaging between and edge applications to enable quick and efficient communications among stakeholders
16	Data usage	• Suggestion to expand/develop the requirements to include secondary uses of the data
17	Identity/ information correlation	• Capability to link parent/child records and family records. May need to link to vital statistics records (birth/death). • Capability to be able to effectively use an agreed-upon list of unique data elements and data identifiers.
18	Persistent data storage	• Functionality to automatically purge/remove data as determined by policy/business rules
19	Record location	• Suggestion to specifically identify the robust set capabilities required of an Record Locator Service (RLS) • Suggestion to expand and clarify requirement to support multiple instances of an RLS, each of which could support different data domains (clinical, lab, claims, etc.) • Capability to combine results of individual RLS' to respond to queries
20	Transient data	• Capability to create ad hoc and specifically requested summary or accumulated data as a result of user defined queries. • Ability to specify (limit) amount of data that can be stored as transient data on the system in terms of volume and size of expected requests

4.   Suggested Next Steps

1. Use the list of requirements listed in Table 4 above as the minimum and essential requirements for each of the ONC-defined 20 functional categories

2. Add the list of requirements listed in Table 5 to fill in gaps in the existing set of functional requirements

3. Need ongoing refinement of "edge" and "core" services for the purpose of articulating functional requirements. Consistent with the purpose of functional requirements, these definitions would be couched in strictly business-oriented language and would not constrain the architecture or the design in any way.

4. It would be helpful to organize functional requirements by business functions. This would assist business stakeholders to understand the requirements from their own perspective and offer a way for demonstrate that these requirements (those found in Tables 4 & 5 above) are truly minimum and essential (while at the same time avoiding system-oriented, implementation-constraining statements of the requirements).

Appendix A. Nationwide Health Information Network Functional Requirements

Appendix A is provided as a separate document to provide the best legibility. This document lists each individual functional requirement and along with comments regarding their inclusion in the minimum and essential set of requirements.

Appendix B. NHIN Mapping of Functional Categories by Aggregate Categories

Table 6: Mapping of Functional Categories to Aggregate Functional Categories

Aggregate Functional Categories	Functional Categories
Data Content	Data Content
	Data Quality/Integrity
	Data Source
	Data Usage
Data Storage	Persistent Data Storage
	Transient Data Storage
Data Transaction	Pull
	Push
	Audit and Logging
	Data Access and Update
	Data Routing
	Data Transaction Verification
Data Transformation	Data Filtering
	Data Mapping/Translation
	Data Rendering
Information Location	Identity/Information Correlation
	Record Location
Security	Authentication
	Authorization
	Confidentiality
	Credentialing

Acronyms

AHIC	American Health Information Community
AHRQ	Agency for Healthcare Research and Quality
CDO	Care Delivery Organization
CHI	Consolidated Health Informatics
CT	Clinical Terminology
DICOM	Digital Imaging and Communications in Medicine
EHR	Electronic Health Record
FHA	Federal Health Architecture
FISMA	Federal Information Security Management Act
HIPAA	Health Insurance Portability and Accountability Act of 1996
HL7	Health Level 7
HSPD	Homeland Security Presidential Directive
IEEE	Institute of Electrical & Electronics Engineers
IT	Information Technology
LOINC	Logical Observation Identifier Name Codes
NHIN	Nationwide Health Information Network
NIST	National Institute of Standards and Technology.
NPI	National Provider ID
ONC	Office of the National Coordinator for Health Information Technology
PHR	Personal Health Record
RDL	Randomized Data Linker
RLS	Record Locator Service
RBAC	Role Based Access Controls
SOX	Sarbanes-Oxley Act of 2002
SNOMED	Systematized Nomenclature of Human Medicine
SSO	Single Sign-On

List of References

1. *NCVHS Discussion Template of NHIN*; July 14, 2006

2. *Summary Comments – FHA Review of the Nationwide Health Information Network Functional Requirements*; Version 3.0; June 26, 2006

3. *Nationwide Health Information Network Functional Requirements*; Version 3; April 16, 2006

4. *Harmonized Use Case for Biosurveillance (Visit, Utilization and Lab Result Data)*; March 19, 2006

5. *Harmonized Use Case for Consumer Empowerment (Registration and Medication History)*; March 19, 2006

6. *Harmonized Use Case for Electronic Health Records (Laboratory Result Reporting)*; March 10, 2006

7. *Health Information Exchange (HIE)* located at http://www.ahrq.gov/data/infostd1.htm

8. *Healthcare Informatics Standards Activities of Federal Agencies (A Compendium)*, September 1996, Sponsored by Center for Information Technology, Agency for Health Care Policy and Research located at http://www.va.gov/publ/standard/healthfed/toc.htm