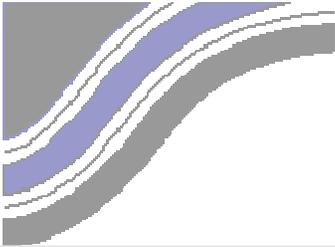




The National Committee on Vital and Health Statistics
The Public Advisory Body to the Secretary of Health and Human Services



Functional Requirements Needed for the Initial Definition of a Nationwide Health Information Network (NHIN)

Simon P. Cohn, MD

Associate Executive Director, The Permanente Federation, Kaiser Permanente
Chair, NCVHS and Ad Hoc Workgroup on NHIN

Harry Reynolds

Vice President, Blue Cross Blue Shield of North Carolina
Vice-Chair, NCVHS Ad Hoc Workgroup on NHIN

NCVHS

- Statutory public advisory body to the Secretary of Health and Human Services
 - 57 year history of advising HHS in the areas of health data, health statistics, privacy and national health information policy
- 18 members
 - 16 appointed by the Secretary, 2 by Congress
 - Leaders and experts in their fields
- Reputation for open, collaborative processes and ability to deliver timely, thoughtful, and practical recommendations

Outline

- Charge to the NCVHS
- NCVHS Observations
- NCVHS Recommendations
- High Level Minimum but Inclusive Functional Requirements for a NHIN
- Gaps, Policy Issues, and Needed Standards
- Next Steps

NCVHS Charge

- The NCVHS has been asked by ONC to review and synthesize the results of the June 28-29 Forum and the functional requirements identified by NHIN prototype consortia contractors,
 - to define a minimum, but inclusive, set of functional requirements necessary NHIN activities
 - wrapped in a privacy and security structure that warrants the trust of the individual whose information is exchanged.
 - These requirements should not include architectural decisions.

NCVHS Ad Hoc Work Group on NHIN

Chair: Simon P. Cohn, M.D., M.P.H. Kaiser Permanente

Vice Chair: Jeffrey S. Blair, M.B.A. Lovelace Clinic Foundation

Vice Chair: Harry Reynolds Blue Cross Blue Shield of North Carolina

John P. Houston, J.D. University of Pittsburgh Medical Center

Stanley M. Huff, M.D. University of Utah

Mark A. Rothstein, J.D. University of Louisville School of Medicine

Paul Tang, M.D. Palo Alto Medical Foundation

Kevin C. Vigilante, M.D., M.P.H. Booz-Allen & Hamilton

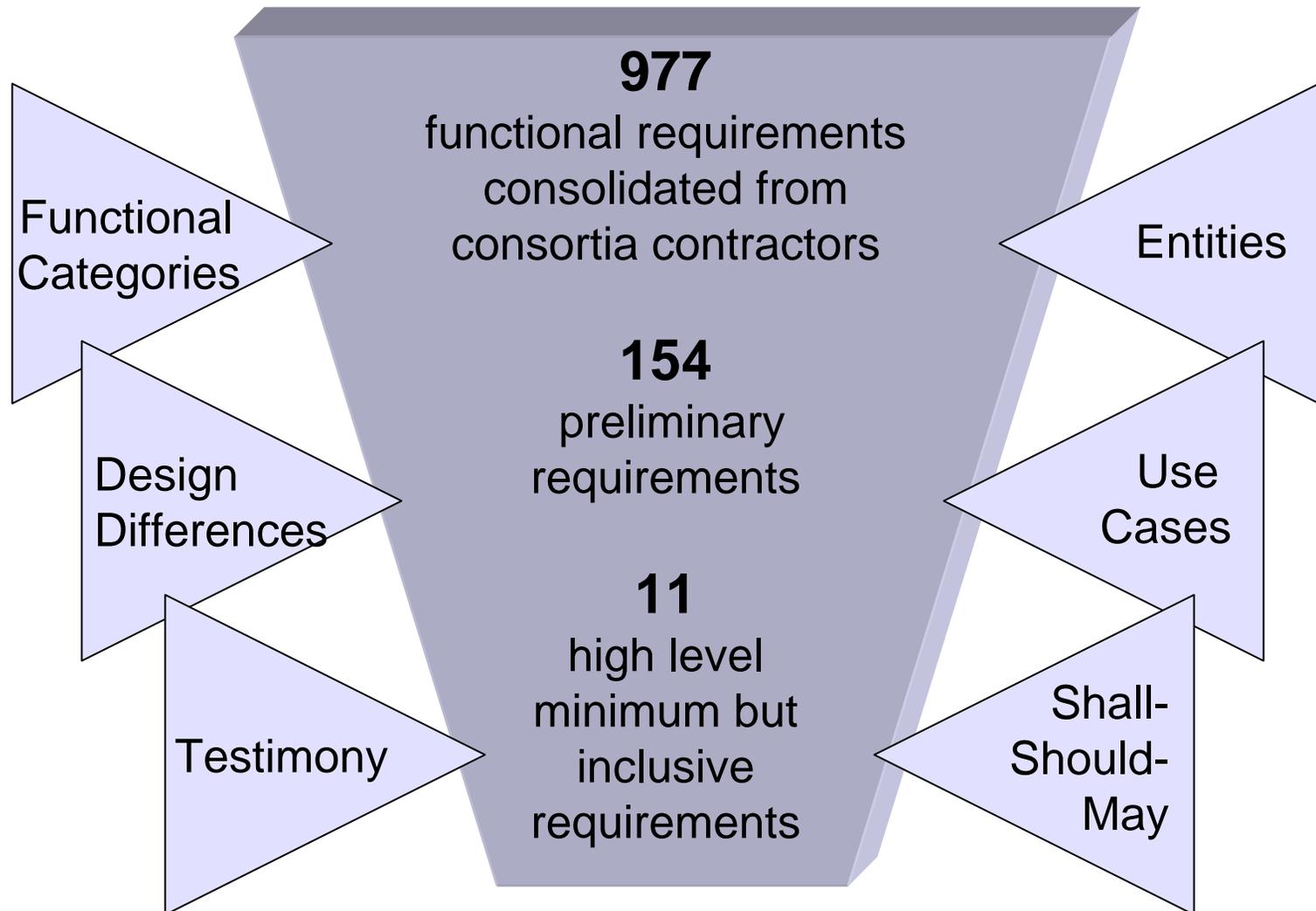
Judith Warren, Ph.D., RN University of Kansas School of Nursing

Lead Staff: Mary Jo Deering NCI

NCVHS Process

- Participated in NHIN Forums on June 28-29 and Oct. 16-17, 2006
- Held public hearings in Washington, DC:
 - June 29, 2006
 - July 27-28, 2006
- Held open public conference calls:
 - August 31, 2006
 - October 3, 2006
- NCVHS Full Committee scheduled to vote on report, October 30, 2006

Refinement of Functional Requirements



NHIN Perspective

- “A nationwide health information network that can provide low-cost and secure data movement” is a key strategy for interconnecting health care.
(www.hhs.gov/healthit/framework.html)
- “As the nation embarks on the widespread deployment of EHRs, a key consideration will be the ability to exchange patient health information accurately and in a timely manner under stringent security, privacy, and other protections”
(www.hhs.gov/healthit/nhin)

NHIN Activities

- Many tasks in the initiative to create a nationwide health information network
 - Prototype development, consortia contractors
 - Standards, HITSP
 - Certification, CCHIT
 - Functional requirements, NCVHS
 - Policy and transport agreements
- See also: NCVHS Report June 22, 2006 on “Recommendations Regarding Privacy and Confidentiality in the Nationwide Health Information Network” (www.ncvhs.hhs.gov)

Observation

A nationwide health information network is not a specific entity, but a ***system of systems . . .***

Functional requirements are about the entire initiative - not specific to an entity

Differences in Design

- Prototype consortia contractors and other testifiers have proposed a variety of different ways systems may interact and interconnect with one another
- These differences (“architectural variations”) may exist because of:
 - Different business cases and policy needs
 - Varying maturity (or lack thereof) in standards and technology

Recommendations

- The NCVHS recommends that HHS adopt the set of minimum but inclusive high level functional requirements for the initial definition of a nationwide health information network
 - Where variations exist and seem to be compatible with one another and do not impose an undue burden, the NCVHS includes them in the minimum but inclusive requirements
 - Where variations exist, but appear to be incompatible or impose undue burden, the NCVHS recommends further study to reconcile incompatibilities
- The NCVHS also makes recommendations relative to specific gaps, policy issues, and needed standards



High Level Requirements

- 1. Certification**
- 2. Authentication**
- 3. Authorization**
- 4. Person Identification**
- 5. Location of Health Information**
- 6. Transport and Content Standards**
- 7. Data Transactions**
- 8. Auditing and Logging**
- 9. Time-sensitive Data Access**
- 10. Communications**
- 11. Data Storage**

Functional Requirements

1. Certification: Utilize a certification process that includes the requirements (standards and agreements) with which any entity's health information users must conform for exchange of data within a nationwide health information network.

- 1.1 Certification of an entity's ability to connect with a nationwide health information network should include a description of the level of participation for which an entity's information systems are capable. For example, a small provider may only be able to exchange data within a nationwide health information network via a gateway; another entity may only be able to exchange certain types of data electronically, or during certain hours.

Functional Requirements, Con't.

2. Authentication: Enable authentication of an entity's users (systems, software tools, and individuals) as well as independent users whenever location of information and/or data are exchanged within a nationwide health information network.

- 2.1 Enable an entity to register (provide authorization and establish authentication processes for)[1] users to connect with a nationwide health information network in a manner consistent with all HIPAA and other applicable federal, state, and local privacy and security legislation/regulation.
- 2.2 Protect authentication credentials during transmission.
- 2.3 Provide mechanisms for non-repudiation when the policies of the parties exchanging data would require such service.

Functional Requirements, Con't.

- 3. Authorization:** Facilitate management of an individual's permission/authorization to share information about location of health information or apply restrictions on access to specified health information.
 - 3.1 Enable entities and/or users to provide permissions, authorizations, and/or restrictions to share location information/data.
 - 3.2 Enable changes to be made in permissions, authorizations, and restrictions as requested by applicable entity and/or user.
 - 3.3 Allow access to location of information and/or data based only on permission/authorization status or emergency access as defined by law.
 - 3.4 Utilize standard authorization codes to convey permissions/authorizations to share data.

Functional Requirements Con't.

3. Authorization, Con't.

- 3.5 Enable participants in a nationwide health information network the ability to anonymize and re-link data to ensure its confidentiality, in accordance with policies of the relevant entities (e.g., public health departments).
- 3.6 Enable an entity to de-identify and aggregate data, for research or other purposes, upon request

4. Person Identification: Utilize a standard person identity/information correlation process to uniquely identify an individual.

- 4.1 Uniquely identify an individual through matching on a common set of various identifiers, such as last name, middle name, first name, date of birth, gender, etc.
- 4.2 Utilize a set of standard policies to resolve identity ambiguities, consistent with applicable tolerance levels for errors.

Functional Requirements, Con't.

5. Location of Health Information: Provide functionality that will locate where health information exists for identified individuals.

- 5.1 Utilize a standard, unique entity identifier (such as the ISO Object Identifier [OID] recommended by HITSP) to locate entities holding a specific individual's information.
- 5.2 Provide notification concerning location of information, pointers to the locations, metadata describing the nature of available data (e.g. radiology report, dates of service, advance directives), or the data itself to the requestor depending on the structure of the network used and agreements in place.
- 5.3 Provide information back to the authorized requestor if identity, location information, and/or data could not be determined and/or provided.

Functional Requirements, Con't.

6. Transport and Content Standards: Transport requests for and their responses to location of information, requests for data, data itself, and other types of messages (such as notifications of the availability of new data) to destinations using general industry-recognized transport types (e.g., Internet Protocol Version 6 [IPv6]) and authorized recipient's specified mode (e.g., e-fax vs. transaction) to and from electronic addresses that are unambiguously identified in a standardized manner.

6.1 Support content (vocabulary and code sets), application protocols, and message formats used for the exchange of health information within a nationwide health information network that conform to standard interoperability specifications.

Functional Requirements, Con't.

6. Transport, Con't.

- 6.2 Verify the integrity of data transmission using general industry recognized methods.
- 6.3 Enable standard information metadata (e.g., UML, XSD) to be included in message formats in order to convey, for example, sensitivity restrictions, individual permissions, and entity preferences.
- 6.4 Support the ability to include an error message service that notifies the requestor if authentication or authorization is not verified.
- 6.5 Support, based on an entity's query, the ability to temporarily hold and aggregate appropriate error messages or data until completely collected and ready for transmission to the requestor.

Functional Requirements, Con't.

6. Transport, Con't.

- 6.6 Support the ability to transport data, as directed, from one entity's system to another, such as from one personal health record to another personal health record, or from one provider's system to a personal health record.
- 6.7 Provide the ability to send/receive/retransmit acknowledgment of data requests or data content transmissions.
- 6.8 Enable entities and systems to transport updates, corrections, and amendments to health information in accordance with HIPAA requirements and internal policies.
- 6.9 Ensure that all parties involved in the transport of health information manage the connections with contingency plans, security incident procedures, ongoing evaluation and risk management, and retention of data and metadata (including audit logs) as required by state statutes and other requirements.

Functional Requirements, Con't.

7. Data Transactions: Provide functionality that will enable data transactions to occur among authorized entities and/or users upon specific trigger events, such as to automatically send final lab results for any previously sent preliminary results, send any changes in medications prescribed, report medication errors, notify public health about the occurrence of a bio-hazard event, inform individuals about the availability of a clinical trial, determine hospital census for disaster planning, etc.

- 7.1 Identify the source of any externally-provided data in whatever form the data may take (e.g., aggregated, anonymized, or identifiable).
- 7.2 Enable data filtering to allow for subscription and un-subscription to specified or all available future clinical events data.

Functional Requirements, Con't.

7. Data Transactions, Con't.

- 7.3 Enable entities to acquire data to monitor a previously detected event, generate alerts/notifications, or perform similar functions.
- 7.4 Enable entities to account for disclosures in accordance with HIPAA requirements if a covered entity; or provide an audit trail of accesses and disclosures if not a covered entity.
- 7.5 Support consistent methodology for granting and tracking access in applicable emergency situations (e.g., when normal authorizations for access are not feasible and special procedures are instituted to gain access to critical care data).

Functional Requirements, Con't.

8. Auditing and Logging: Log and audit all (intentional or unintentional) connections and disconnections to network services and all network configuration changes, generating alerts/notifications for system activity outside the normal range of monitoring levels/thresholds.

- 8.1 Retain logs for period of time determined by law, accrediting agencies, marketplace, and entities.
- 8.2 Protect audit data from unauthorized access/modification.
- 8.3 Generate evidence to support incident management (investigations) and response processes (corrective action).
- 8.4 Be guided in standards and policy adoption by regular risk assessments.

Functional Requirements, Con't.

9. Time-sensitive Data Access: Enable time-sensitive data request/response interactions to specific target systems (e.g., query of immunization registry, request for current medication list).

10. Communications: Communicate health information using HITSP-identified standard content and message formats.

- 10.1 Enable mapping between versions of a standard and multiple standards, mapping terminologies and code sets, and supporting Americans with Disabilities Act Section 508 compliance.
- 10.2 Support display, entry, or retrieval of data in multiple ways as determined by the needs of the recipient.

Functional Requirements, Con't.

11. Data Storage: Enable the ability to aggregate data from disparate sources to facilitate communications. For example, temporarily hold information as it is being collected to communicate a concise summary of the information; or permanently store data from uncoordinated sources across time to support a data registry.

Gaps

- The original functional requirements addressed 3 use cases
- The NCVHS recommends that HHS support the testing of the high level functional requirements against other very common use cases. These might include:
 - E-prescribing
 - Medication reconciliation
 - Use of clinical decision support
 - Chronic care, long term care, home health care, behavioral health care, and other settings for care
 - Reimbursement for healthcare services
 - Clinical research
 - Regulatory reporting
 - Selected services provided by public health departments
 - Others to be identified

Policy Issues

- a. Utilize the results of the prototypes and growing community of experience in health information exchange to determine the public policy that describes where responsibilities for the performance of the various functional requirements may exist within a nationwide health information network
- b. Determine how to assure ongoing conformance of entities and their systems to the requirements for connectivity and exchange of data
- c. Identify and recommend policy to ensure accurate matching of individuals to their health information
 - Individual identification
 - Health information location
- d. Support use of standards that would enable communication of individual permissions or entity preferences concerning specific data

Policy Issues, Con't.

- e. Recognize that baseline requirements for privacy, security, transactions and code sets, and identifiers are provided for by HIPAA for covered entities, but that equivalent requirements do not exist where there may be exchange of health information among non-covered entities or their business associates. Privacy measures at least equal to those in HIPAA should apply to all personal health record systems
- f. Collaborate with other public and private entities to develop a public awareness campaign

Standards Needed

- a. Authorization codes that support individuals' permissions
- b. Provider preference codes, such as a provider wants to receive automatic updates
- c. Clinical terminology subsets and cross-maps for multiple use cases
- d. Metadata requirements for patient consent documents and processes
- e. Metadata related to retention of clinical data and queries for clinical data in multiple use cases
- f. Information location/identity correlation processes, including registry services

Standards Needed, Con't.

- g. Content standards for certain types of messages, especially relating to event detection and alerts/notifications
- h. Implementation guides for electronic clinical documents and messages
- i. Managing the shared use of unique identifiers across multiple participating institutions
- j. Processes and specifications for correction of existing clinical information

Recommended Next Steps for HHS

- a. Use the high level functional requirements as described in this Report as a way to communicate the nature of the initiative that is enabling a NHIN
- b. Utilize more detailed statements of functionality to illustrate specific use cases and business needs, especially with respect to the use of the data for clinical care by external providers and to enable use by safety net organizations
- c. Monitor the emergence of types of entities that enhance the adoption of a NHIN and any issues encountered

Comments?

- By:
 - Wednesday, October 18, 2006,
Close of Business Eastern Time
- To:
 - Simon.Cohn@kp.org
 - MargretCPR@aol.com