NATIONAL COMMITTEE ON VITAL AND HEALTH STATISTICS

Report to the Secretary
of the U.S. Department of Health and Human Services

on

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

DRAFT
September 20, 2006

Report to the Secretary of HHS

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

Table of Contents

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

Introduction

Purpose and Scope

The National Committee on Vital and Health Statistics (NCVHS) was asked by the Office of the National Coordinator for Health Information Technology (ONC) to identify minimum but inclusive functional requirements needed for the initial definition of a nationwide health information network (NHIN).

In describing a nationwide health information network, the ONC observed that "as the nation embarks on the widespread deployment of EHRs [electronic health records], 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).

A nationwide health information network is not a single entity, but a system of systems. It is envisioned that such a network would provide for the secure exchange of health information for many uses in multiple ways and by a number of different health information network providers. There are many tasks to be performed to see that a nationwide health information network initiative is achieved. These tasks include creating policies, standards, and transport agreements. Identifying a set of minimum but inclusive functional requirements is one of those tasks. This set must be "minimum" insofar as it establishes basic requirements, but must be "inclusive" because it is possible that some of the requirements may be performed in multiple ways.

NCVHS has addressed other issues required for a secure and effective NHIN in other reports to the Secretary of Health and Human Services. In particular, privacy was covered in the June 22, 2006 letter report entitled, "Recommendations Regarding Privacy and Confidentiality in the Nationwide Health Information Network." These and other NHIN-related recommendations are not repeated in the current report, but readers are encouraged to visit the NCVHS Web site (http://ncvhs.hhs.gov).

Background

On November 15, 2004, the ONC released a Request for Information (RFI) that sought public comment regarding how widespread interoperability of health information technologies and health information exchange can be achieved through a nationwide health information network initiative. Substantial comments were received from over 500 organizations and individuals. These were analyzed and summarized into a report posted to the Web on June 3, 2005 (see www.hhs.gov/healthit/rfisummaryreport.pdf). On June 6, 2005, HHS published a Request for Proposals (RFP) for the development of prototypes for a nationwide health information network. Four awards to consortia were announced on November 10, 2005. In [May 2006], the four consortia contractors submitted lists of NHIN functional requirements, which were consolidated into a non-duplicative list of 997 and discussed at a NHIN Forum on June 28-29, 2006.

The NCVHS Process

To identify the minimum but inclusive functional requirements for the initial definition of a nationwide health information network, the NCVHS used a process of refinement that started with the initial set of consolidated functional requirements.

Over the course of the summer, the NCVHS heard significant amount of public comment that contributed to this report. The NCVHS participated in the NHIN Forum on June 28-29, 2006, held public hearings on June 29 and July 27-28, 2006 in Washington, DC, and held public conference calls on August 31 and October 3, 2006 to receive comments on preliminary documents and drafts. In addition, working documents were posted on the Web for further contributions. Although time for input was short, the NCVHS is very appreciative of the effort so many put into contributing comments. Members of the NCVHS are listed in **Appendix A** and testifiers are listed in **Appendix B**.

The process to analyze and develop a list of high level minimum but inclusive functional requirements needed for initial definition of a nationwide health information network was aided by an enumeration of Functional Categories provided by ONC. The list of ONC Functional Categories and their definitions is provided in **Appendix C**.

The process used to achieve the recommendations for the set of high level functional requirements included analysis of the original 977 detailed functional requirements, consolidation of those 977 requirements into a working set of minimum but inclusive set of functional requirements, and then refinement of the working set into high level functional requirements. The high level functional requirements are summarized in **Figure 1** (on page X). A map of the high level functional requirements to the ONC Functional Categories is provided in **Appendix D**.

To review the working material, readers are referred to Appendices E, F, and G. An introduction to the analysis of the original 977 requirements and a spreadsheet of the requirements are provided in **Appendix E**. The interim working set of functional requirements and gaps identified by testifiers is provided in **Appendix F**. A map of the high level functional requirements to the interim working set of functional requirements is provided in **Appendix G**.

Intended Audience

This report is intended for a broad audience. The Framework and High Level Functional Requirements should serve all readers in achieving a general understanding of the concept and end-to-end capabilities of a nationwide health information network. The High Level Functional Requirements may serve as a checklist for organizations[1] to assure they are considering all critical elements for connecting to a nationwide health information network. They may also serve as a description of services to be developed by network service providers and other intermediary entities. The Description of Gaps, Policy Issues, and Needed Standards should assist those with more specific tasks associated with developing the framework for a nationwide health information network initiative. For example, they should be useful for ONC in addressing specific policy issues. The Health Information Technology Standards Panel (HISTP) may find the identification of needed standards helpful in advancing their development. The Certification

[1] Organizations may include sub-network organizations, regional health information organizations, connected communities, and others.

Commission on Health Information Technology (CCHIT) may find the minimum but inclusive functional requirements can contribute to development of certification criteria.

Framework

Importance of a Nationwide Health Information Network

There is significant evidence of the need for a nationwide health information network. The consortia contractors used three scenarios, or use cases, to focus the initial effort and illustrate how a nationwide health information network would be used. Each of the three scenarios – named EHR-Lab, Consumer Empowerment-Personal Health Record, and Bio-Surveillance – focused on a number of goals. There are literally thousands of uses of health information – for direct patient care, many forms of consumer empowerment, public health, case management, disease management, reimbursement, clinical research, and many others. However, most health information is exchanged in one of three ways: via document sharing, transactions, and to a lesser, but perhaps more desirable extent, dynamic queries.

The following scenarios further illustrate the current state of health information exchange and how a nationwide health information network would improve such exchange:

- A physician's office may have an arrangement with an e-prescribing gateway to route prescriptions to pharmacies of a patient's choice. Each prescription transaction received by the gateway can be transformed into the format required of the recipient pharmacy or to meet specific legal requirements (e.g., a particular version of a standard transaction or an e-fax of a prescription requiring a wet signature). However, with a nationwide health information network, adverse drug event reporting could be automated for earlier detection of drug problems.

- After a local disaster, an emergency department treating an unconscious, but identifiable, patient may be able to view a list of current medications consolidated from a pharmacy benefits management system, but not be able to identify the patient's primary care physician or retrieve data from the office's EHR. If the patient is not local or is displaced as a result of the disaster, a nationwide health information network would enable other providers to access critical health information.

- A patient with multiple health conditions may visit several health care providers, each time completing a patient history form. Each time, however, the patient may record some information and not other information. With a personal health record maintained within a nationwide health information network, the patient can compile healthcare events as they occur. This enables a complete health picture to be available to any or all providers as the patient so chooses.

- A school may query a statewide immunization registry to check that a child's shots are up-to-date. The registry may have received the immunization data from a batch transaction sent by a health insurer where the child is enrolled, from a paper fax sent by a physician's office, and/or from a direct posting by the child's parent to a Web site maintained by the registry. A nationwide health information network can support services that ensure that the three reports actually do belong to one specific child and that they are not counted three separate times. In addition, it can enable the de-

identification of the data to report aggregate immunization rates to the state's public health department.

In addition to the specific potential benefits reflected by these and other scenarios, a nationwide health information network can also address needs relative to security services, privacy protections, and methods to identify (or de-identify) individuals who are the subject of the health information exchanged. During 2005-2006, the NCVHS held six hearings on the topic of matching patients to their records. A summary of the testimony is provided in **Appendix H**. The NCVHS learned, for example, that today every entity utilizes a different process to identify individuals, and a different set of data elements to match individuals to specific information. There are both privacy and health care reasons for the need to assure the unique identity of an individual. In addition, there are very few environments today in which there are organized means to identify where health information may exist as applicable to a given, authorized use. There is a significant need for services to improve the exchange of health information in a purposeful manner and with the utmost of privacy and security protections. Health care quality, patient safety, public health and bio-surveillance, research, and other appropriate uses of health information would be greatly enabled by the ability to easily exchange health information.

Observations Related to a Nationwide Health Information Network

System of Systems

A nationwide health information network is not a specific entity – it is a system of systems. Given that a system is a collection of parts that work together to achieve a common purpose or carry out a specific goal, a system of systems may include any number of systems, each with its own goal or set of goals.

Services, Functions, and Functional Requirements

Within a nationwide health information network, various systems would provide services to enable health information exchange in a secure and protected manner. Some of these systems may reside in specific healthcare entities. For example, a hospital may be able to perform a translation service that enables it to format its own standard transactions. Other services may be offered by network service providers. For example, a physician's office may need an e-prescribing gateway service to route prescriptions to pharmacies of the patient's choice. Vendors may have systems that provide personal health record services. Various community organizations may support systems offering terminology mapping or record location services.

A key provision of a nationwide health information network, however, would be that there are agreed upon policies, standards, and transport arrangements for any entity to provide or use such services and participate in such exchanges. The **functions** that various **services** need to provide constitute the **functional requirements** for a nationwide health information network. Functions are actions, activities, or work. Services are the act of supplying such work, and imply taking into account the social, political, and organizational factors of supplying the work. Functional requirements identify what functions service providers must supply.

Differences in Design of Services (Architectural Variations)

As a nationwide health information network is being developed and prototyped in different locations, a number of different ways systems may interact and interconnect with one another are being proposed. There are differences in business cases and policy needs. Some differences reflect the maturity or lack thereof in standards and technology. Differences in how services are provided within a nationwide health information network have been described by ONC as architectural variations. Information flow variations within several of the ONC Functional Categories are described in **Appendix I**. The NCVHS has analyzed these variations and where they appear to be compatible with one another, the NCVHS recommends the variations be accommodated to the extent possible. Where variations may be incompatible with one another, however, the NCVHS recommends further study to determine how variation can be reduced.

Discussion of Terms

In identifying the minimum but inclusive functional requirements for a nationwide health information network, terms used and how they are defined play a critical role in their framing. Special attention has been given to the following terms or sets of terms as the minimum but inclusive functional requirements are described (in the next section of this report):

- **Entities, systems, and users:** There are many **entities** that will use a nationwide health information network; and there are many entities that will supply services for networking. Some entities will be both users and suppliers. Entities may include care delivery organizations, consumer systems, data analysis and secondary use systems, payer systems, health information intermediaries, and network service providers.

  Within these broad entity descriptions, many more specific types of entities can be described. Certainly care delivery organizations may include hospitals, clinics, physician offices, long term care facilities, home health agencies, institutional infirmaries, and others. Consumer systems are perhaps newer, but include those both “tethered” and “un-tethered” to a care delivery organization. Data analysis and secondary use systems may include clinical researchers, pharmaceutical manufacturers, government agencies, accreditation organizations, and many others. Payer systems may include insurers, health maintenance organizations, group health plans, and other organizations that support payers, such as pharmacy benefits managers and case management companies. Health information intermediaries may include healthcare clearinghouses, e-prescribing gateways, and other types of intermediaries. There are also entities that are more closely aligned with specific types of services that enable participation in a nationwide health information network. These may provide message handling, record location, terminology mapping services, etc. Finally, some entities may provide many network services for a specific group of entities, such as sub-network organizations, regional health information organizations, connected communities, and others.

  The purpose of enumerating these entities is to emphasize that there are many players that constitute a nationwide health information network. In short, this document does not suggest that there is a single entity performing all the services of a nationwide health information network.

  Likewise, although initial prototype development focused on three scenarios, or use cases, there is no intent to preclude any specific type of legitimate use or user. **Users** may be individuals, software tools, or other **systems**. Individuals, in particular, may have many roles. Some special roles are typically identified within the healthcare industry.

These include members of the workforce in HIPAA-covered entities, such as providers (which may be used to describe a clinician or a healthcare organization authorized to bill for healthcare services), health plans, and healthcare clearinghouses. In addition, all individuals have some health information; and at various times may be patients, consumers, clients, residents, inmates, beneficiaries, etc. Other individuals who may also have legitimate access to health information include personal representatives of patients, caregivers (generally not healthcare professionals and not always personal representatives), and the workforce of many other organizations, some of whom are designated by HIPAA as business associates of covered entities and others who may derive their authority for access to health information through legal and regulatory processes. In the context of identifying minimum but inclusive functionality for entities to participate in a nationwide health information network, there is an attempt made to use the terms entity, system, and user as referring to an organizational construct, information system (which may also be a user), and individual respectively.

- **Data, information, and record**: The industry often uses these terms synonymously, and other times use them to convey different meanings within different contexts.

  Within the context of the original functional requirements, the term **data** seems to refer to any health information associated with a specific individual that would generally be considered confidential and/or sensitive. HIPAA-covered entities would consider such data protected health information (PHI), but in a broader context, it may include any data that an individual considers confidential or sensitive. This may include health information that is not held by a covered entity whose duty it is to protect the health information. It may include identifying information, such as an individual's address or a provider's DEA number, that – if stolen – could result in harm.

  In analyzing the functional requirements, it is observed that the term "information" is not only used interchangeably with (confidential and/or sensitive) data, but also to describe generally available information that is not confidential or sensitive, such as information about the existence of a clinical trial, properties of drugs, hospital census, etc. This more limited use of the term seems inconsistent with its more general definition, where **information** is the result of associating data within a context to provide knowledge.

  The term **record** is used in the original enumeration of functional requirements as suggesting a location or collection of data. The data contained in the record may or may not be known to the service that is attempting to locate health information on an individual. Whether this was the actual intent or not, for purposes of this report, every attempt is made to treat data, information, and record, unless otherwise specified, as being confidential and/or sensitive in some way. Furthermore, privacy and security protections ought to be afforded whether the data, information, and record are considered "protected health information" under HIPAA or not.

- **Data quality and data integrity**: These terms appear to be used grouped together in the original ONC categorization of functional requirements. Typically, **data quality** is a property associated with the completeness and accuracy of the data captured and subsequently processed into information. The quality of data and any resultant information may be ascertained by various validity and reliability checks. Alternatively, **data integrity** generally refers to the property of data as being whole or unimpaired. This generally refers to maintaining the technical representation of data and information within

an information system and as it is transmitted across information systems. Evaluating the integrity of data is generally a technical function.

- **Pull vs. push**: Much of the functionality described for entities to participate in a nationwide health information network relates to requests for data (**pull**); however, there are also a number of specific use cases that require data to be sent to an entity where a specific request for data may not have been made, but where a subscription arrangement or expectation exists that such data will be pushed to it (**push**). Specific examples include sending new event information to a previous requestor of lab results, supporting medical supplies inventory and resource management data communications to public health, enabling patients and clinicians to report adverse medical events and/or errors to FDA, enabling individuals to find and enroll in appropriate clinical trials, and providing data to and receiving data from payer systems in support of eligibility verification, billing, and other administrative services. The nature of the data itself and whether it is pulled or pushed is distinguished in the minimum but inclusive functionality only if there appears to be a key difference in functionality, or where some examples would help clarify intent of functionality. Otherwise, pull and push are considered data exchange.

- **Certification, registration, credentialing, evaluation, and testing**: Consortia contractors have used the term **certification**, with respect to information systems, as a process performed to establish the extent to which a particular system, network design, or application implementation meets a pre-specified set of requirements. Consortia contractors use the term **registration** in describing the process of adding a user to a system. The process includes establishing the user's identity, providing a means to authenticate to the system (e.g., password or token), and assigning access privileges based on what the user is authorized, or permitted, to do within the system. ONC has defined the term **credentialing** as a process that provides for validating or confirming the qualifications of licensed professionals, distinct from authentication and authorization. However, some usages of the term credentialing in the detailed functional requirements suggest that it is a process synonymous with authentication and authorization. Since the term credentialing within health care refers to a specific process of reviewing and validating the qualifications of physicians and other licensed practitioners for granting medical staff membership to provide patient care services, the term credentialing has been reserved for this meaning exclusively. The term registration is used instead. Evaluation and testing are actions that may be performed for many different purposes. For example, they may be performed as part of system certification, or to determine whether an implementation conforms to a standard. There is a distinction, however, that the NCVHS observes between evaluation and testing, where **evaluation** suggests a process of inspection, where **testing** refers to an actual trial use.

- **Authorization, restriction, authentication, access controls, and nonrepudiation**: These terms work together to provide confidentiality and security, but each has a specific role in these functions. It is important to recognize these functions when applying these terms in various contexts. **Authorization** is the granting of permission. From the perspective of the individual who is the subject of health information (the subject), the permission is given to the recipient of the confidential information to use and disclose in a manner consistent with the individual's expressed privacy rights and applicable regulations. Such authorization may carry specific **restrictions**, such as not to disclose any health information to certain individuals or entities or to limit health information disclosure in some way. From the perspective of individuals and entities who are the recipients of the subject's confidential health information, authorization is the permission

to carry out uses and disclosures consistent with the Subject's permissions and applicable regulations.

When health information is collected and stored in an information system, **access authorization** is the granting of access to use electronic systems. Access authorization is based on policies and procedures relating to a user's "need to know." The technical administration of access authorization is **access controls**. Access controls and restrictions must operate together. **Authentication** is a process of proving the identity of a system or individual. Authentication establishes the validity of a transmission, message, or originator and verifies the system's or individual's authorization for its use. **Nonrepudiation** is a cryptographic process created so that an author of a message in an information system cannot falsely deny sending the message. With respect to electronic signatures used in authentication, it is proof that only the specific user could have created a specific signature.

- **Anonymization and re-linking.** These functions are used by public health and other entities to remove common identifiers (**anonymization**) and assign a code to a set of health information to enable it to be **re-linked** to other health information with the same code. This process protects individuals' identities, but assures proper counting of cases, especially for bio-surveillance purposes.

High Level Minimum but Inclusive Functional Requirements Needed for the Initial Definition of a Nationwide Health Information Network

Organization

The following high level minimum but inclusive functional requirements are organized as they may be performed by an entity participating in a nationwide health information network. For example, an entity would first be certified to connect to a nationwide health information network. Users (individuals and systems) would need to be authorized to use various systems in specific ways. They would be registered as system users. For any authorized use, the systems and/or individuals would authenticate themselves to a network.

It is important to note that there are differences in how the services meeting these functional requirements might be carried out. Several variations were described by the consortia contractors. In addition, testimony provided to the NCVHS described further variations and stressed the importance of being sensitive to local needs, while recognizing it is not possible to accommodate all variations.

Accommodation of Differences in Design of Services

To address differences in design of services (architectural variations), the NCVHS has structured its description of the minimum but inclusive functional requirements both to recognize variations and to make specific recommendations with respect to the variations:

- Where variations exist and seem to be compatible with one another, the NCVHS describes the variations within the minimum but inclusive set of functional requirements. Many of these variations relate to where functionality may be performed within a nationwide health information network.
- Where variations exist, but they appear to be incompatible with one another, the NCVHS lists the variations and recommends further study to reconcile incompatibilities.

Set of High Level Functional Requirements and Recommendations

The complete set of high level minimum but inclusive functional requirements needed for the initial definition of a nationwide health information network are provided in Figure 1.

Figure 1. Set of Minimum but Inclusive Functional Requirements Needed for the Initial Definition of a Nationwide Health Information Network

1. **Certification:** Utilize a certification process with which any entity's health information users (systems, software tools, and individuals) must conform for exchange of data within a nationwide health information network.

    1.1 Certification of entities connecting with a nationwide health information network should describe the level of participation for which an entity's information systems are capable. For example, a physician's office EHR system may only be available during specified hours to send and receive data; another entity may only be able to exchange certain types of data electronically.
    1.2 The process of certifying entities to exchange data within a nationwide health information network should entail testing of capabilities; and there should be an ongoing systematic evaluation of continued conformance with the certification requirements.

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 policy would require such service.

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

Figure 1. Set of Minimum but Inclusive Functional Requirements Needed for the Initial Definition of a Nationwide Health Information Network Continued

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 HITSP-identified standard authorization codes to convey permissions/authorizations to share data.
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 (HITSP standard) person identity/information correlation process to uniquely identify an individual.

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

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

5.1 Utilize a standard, unique identifier to locate entities holding a specific individual's information.
5.2 Provide notification concerning location of information, pointers to the locations, 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.

6. **Transport 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) and application protocols (message formats) used for the exchange of health information within a nationwide health information network that conform to HITSP interoperability specifications.
6.2 Verify the integrity of data transmission.
6.3 Enable standard information metadata (e.g., UML, XSD, and/or HITSP-specified) to be included in data retrieval or delivery of messages in order to convey, for example, sensitivity restrictions, individual permissions, and entity preferences.

Figure 1. Set of Minimum but Inclusive Functional Requirements Needed for the Initial Definition of a Nationwide Health Information Network Continued

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 the ability to hold and aggregate appropriate error messages or data based on an entity's query.
6.6 Support the ability to move or copy 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 update, correct, and amend health information in accordance with HIPAA requirements and internal policies.
6.9 Ensure that all parties involved in the physical 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 (e.g., as may be provided by HITSP standards).

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
7.2 Enable data filtering to allow for subscription and un-subscription to specified or all available future clinical events data.
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.

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.

Figure 1. Set of Minimum but Inclusive Functional Requirements Needed for the Initial Definition of a Nationwide Health Information Network Continued

8.3 Generate evidence to support incident management (investigations) and response processes (corrective action).
8.4 Conduct regular risk assessments.

9. Dynamic Data Access: Provide for dynamic data access (i.e., time-sensitive request/response interactions to specific target systems, e.g., query of immunization registry) within a nationwide health information network.

9.1 Support consistent methodology for granting and tracking access in applicable emergency situations.

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

10.1 Provide for 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.

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.

Observation: The NCVHS has sequenced these functional requirements assuming a sequential flow. Functional requirements for entities to connect with a nationwide health information network are sequenced first. Functions required to authorize and authenticate users (individuals, software tools, or other systems) are next. Following that are functions required to identify and locate information – whether about a given individual or an aggregate set of data. Lastly identified are functional requirements relating to transporting, securing, aggregating, and retaining health information – whether by a network service provider or an entity itself. Each functional requirement builds upon all predecessor requirements. Hence, for example, transport among systems cannot occur without system authentication; system authentication cannot occur without entity certification; etc..

Global Recommendation: 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, as well as the additional and more specific recommendations following.

1. Certification: Utilize a certification[2] process with which any entity's health information users (systems, software tools, and individuals) must conform for exchange of data within a nationwide health information network.

[2] See definition on page 9.

1.1 Certification of entities connecting with a nationwide health information network should describe the level of participation for which an entity's information systems are capable. For example, a physician's office EHR system may only be available during specified hours to send and receive data; another entity may only be able to exchange certain types of data electronically.

1.2 The process of certifying entities to exchange data within a nationwide health information network should entail testing of capabilities; and there should be an ongoing systematic evaluation of continued conformance with the certification requirements.

Observation: The NCVHS notes that the initial development of network certification criteria is part of the 2007 deliverables from the Certification Commission for Health Information Technology (CCHIT). The NCVHS envisions that the certification process will accommodate appropriate variations by location and system capabilities and enable changes over time. For example, some organizations that provide certification for entities to participate in a nationwide health information network may provide specific services that entities within a local community may desire, such as message handling, terminology mapping, or repository functions. At some time in the future, the entities may prefer to perform these functions themselves.

Recommendation 1: The NCVHS recommends that CCHIT ensure that the network certification currently being addressed accommodate appropriate variations by location and system capabilities and that their ability to change over time is assured.

2. **Authentication:** Enable authentication of an entity's users (systems, software tools, and individuals)[3] 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)[4] 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 policy would require such service.

Observation: Some testifiers to the NCVHS suggested that only local entities should authorize and provide authentication for their users and that authentication should not be a network function. The NCVHS observes that there is a difference between where an entity would authorize and authenticate its own users and where an independent user, such as of a personal health record, would grant authorization to share data and need to authenticate to a network. Variations in where authorization and authentication of systems and individual users – both aligned with an entity and not aligned with an entity – take place seem compatible with the goals of a nationwide health information network. The NCVHS also recognizes that policy matters are the subject of other groups working on the nationwide health information network initiative.

[3] See definition on page 7.
[4] See definition on page 9.

Recommendation 2: The NCVHS recommends that HHS ensure that the current development of policy for participation in a nationwide health information network includes appropriate authorization and authentication processes.

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 HITSP-identified standard authorization codes[5] to convey permissions/authorizations to share data.
    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

Observation: The NCVHS refers readers to its recommendations to the Secretary of HHS on June 22, 2006, "Recommendations Regarding Privacy and Confidentiality in the Nationwide Health Information Network," *regarding an individual's participation in a nationwide health information network. See also recommendations on needed standards later in this report.*

Recommendation 3: The NCVHS recommends that HHS adopt the positions consistent with the NCVHS recommendations of June 22, 2006 regarding an individual's participation in a nationwide health information network, that:

a. "The method by which personal health information is stored by healthcare providers should be left to the healthcare providers.
b. Individuals should have the right to decide whether they want to have their personally identifiable electronic health records accessible via the NHIN. This recommendation is not intended to disturb traditional principles of public health reporting or other established legal requirements that might or might not be achieved via NHIN.
c. Providers should not be able to condition treatment on an individual's agreement to have his or her health records accessible via the NHIN.
d. HHS should monitor the development of opt-in/opt-out approaches; consider local, regional, and provider variations; collect evidence on the health, economic, social, and other implications; and continue to evaluate in an open, transparent, and public process, whether a national policy on opt-in or opt-out is appropriate.
e. HHS should require that individuals be provided with understandable and culturally sensitive information and education to ensure that they realize the implications of their decisions as to whether to participate in the NHIN."

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

[5] To be developed. See Recommendation 14.

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

Observation: Successfully matching individuals to their health information is essential for the functioning of a nationwide health information network. Most entities collecting and maintaining health information have implemented master person indices (MPIs) or an enterprise-wide MPI (E-MPI) to accurately match individuals to their records. A set of demographic data is used for this purpose, although each entity establishes what demographic data and matching process, or algorithm, to use. Although there is a high percentage of correct matching at the entity level, adjudication of non-matches is labor-intensive and time consuming. There are also variations in the need for a perfect match vs. a near-perfect match. For example, the standard tolerance for error may be less stringent for certain kinds of research and administrative uses and much more stringent for healthcare delivery. When two or more entities exchange health information without a standard set of matching data and matching algorithm, the risk of mismatching individuals to their health information increases. Testifiers recommended various automated and manual process for resolving identity ambiguities. The NCVHS observes that the Department of Defense (DoD) and the Veterans Health Affairs (VHA) are working together to test an automated process that results in accurate record matching to enable the transfer of health information from the DoD to the VHA. See also Appendix H.

Recommendation 4: The NCVHS recommends that HHS should identify and recommend minimum criteria for successfully matching individuals to their health information, including that:

a. ONC continue to provide national leadership and direction to the Healthcare Information Technology Standards Panel (HITSP) for the purpose of developing standard criteria for the accurate matching of individuals. The work being conducted by the consortia contractors to identify matching identifiers is one example. The NCVHS stands ready to assist with further analysis of testimony heard during 2005-2006 as well as its experience with vital and health statistics data as another resource.
b. Data sets should be created for use by entities for testing the accuracy of their matching methods.
c. The results of the DoD and the VHA process to accurately match individuals with their health information should be evaluated, including its technical, financial, and social impacts, for adoption within a nationwide health information network.

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

5.1 Utilize a standard, unique identifier to locate entities holding a specific individual's information.
5.2 Provide notification concerning location of information, pointers to the locations, 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.

Observation: The NCVHS observes that there are several entity identifiers in use or being proposed for use within healthcare today, although none are universal and not all available to non-HIPAA-covered entities. HITSP has voted to require ISO Object Identifiers (OIDs) as the sole standard unique organization identifiers that assign and manage patient identifiers.

The NCVHS also observes that in addition to identifiers, there are a variety of processes for location of health information, including those in which the provision of access or retrieval of health information is performed simultaneously with the location of the health information. It further observes that some of the variations relate to whether the subject of the query is a specific individual's health information or other information. Other information may be de-identified and/or aggregated health information. A nationwide health information network may also serve to support the exchange of information not related to or derived from individual health information, such as hospital census information or the availability of a clinical trial at a particular research institution. HITSP has recognized that standards are not completely architecture-neutral and that it may be necessary to define a range of architectural options that is not limitless.

Recommendation 5: The NCVHS recommends that HHS should collaborate with public and private organizations on the development, deployment, and systematic continuing evaluation of services for the location of health information about individuals that would accommodate local preference and system capabilities to the extent feasible, yet be compatible within a nationwide health information network.

6. **Transport Standards:** Transport requests for and 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) and application protocols (message formats) used for the exchange of health information within a nationwide health information network that conform to HITSP interoperability specifications.
    6.2 Verify the integrity of data transmission.
    6.3 Enable standard information metadata (e.g., UML, XSD, and/or HITSP-specified) to be included in data retrieval or delivery of messages 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 the ability to hold and aggregate appropriate error messages or data based on an entity's query.
    6.6 Support the ability to move or copy 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 update, correct, and amend health information in accordance with HIPAA requirements and internal policies.
    6.9 Ensure that all parties involved in the physical 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 (e.g., as may be provided by HITSP standards).

Observation: The NCVHS notes that it is important to recognize that many of the functions associated with transporting meaningful messages depend on the ability of an entity's systems to produce standard messages or that the entity will utilize one or more third parties to process messages into standard formats. Such conformance to standards may be enabled by a network service provider, system vendor, entity itself, or other means. Such variation appears to be compatible with the goals of a nationwide health information network that is deployed in a federated manner.

Recommendation 6: The NCVHS recommends that HHS support the work of the HITSP in promoting creation, adoption, and conformance to message and content standards for use within a nationwide health information network. (See also Recommendation 15 for specific standards gaps.)

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
    7.2 Enable data filtering to allow for subscription and un-subscription to specified or all available future clinical events data.
    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.

Observation: The NCVHS heard testimony from some that a nationwide health information network should only enable retrieval of data based on a specific query (pull). Still other testifiers, however, supported the ability to offer push services that enable, with permission, the ability to inform others of the availability of (new or updated) data and the ability to be notified when certain data become available..

Recommendation 7: The NCVHS recommends that HHS support a nationwide health information network initiative within which both pull and push data transaction services can be accommodated based on local or community policies.

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 Conduct regular risk assessments.

Observation: The NCVHS heard testimony from some that logging and auditing of connections and disconnection to network services are sufficient measures to ensure the security (confidentiality, integrity, and availability) of any network, and from others that access controls alone are sufficient measures to ensure the security (confidentiality, integrity, and availability) of any network. NCVHS believes both are necessary. The absence of auditing and logging is also inconsistent with HIPAA security requirements as they may apply to various entities. In addition to audit and logging being a minimum and essential functionality, other audit and logging functionality were brought forth for inclusion in network functional requirements. These included:

- *Auditing of cross organization data access at the healthcare entity level so that inappropriate data retrieval can be retrospectively identified (the healthcare entity is responsible for auditing the specific provider of care requesting the retrieval).*
- *Auditing of cross organizational data access at the provider of care level through metadata shared by the requesting organization.*

NCVHS Recommendation 8: The NCVHS recommends that HHS support the continued development and testing of approaches for a nationwide health information network that incorporate logging and auditing and access controls.

9. **Dynamic Data Access:** Provide for dynamic data access (i.e., time-sensitive request/response interactions to specific target systems, e.g., query of immunization registry) within a nationwide health information network.

9.1 Support consistent methodology for granting and tracking access in applicable emergency situations.

Observation: The ability to query and obtain a response in real time, at the point of care or to respond to a disaster situation is an essential function of a nationwide health information network that will improve patient care, enhance emergency responsiveness, and reduce medical errors. Access to health information in an emergency situation, however, must be performed within stringent security controls that enable access only when legitimately required and afford special monitoring of those accesses.

Recommendation 9: The NCVHS recommends that HHS support the capability of a nationwide health information network that enables dynamic data access, especially within a construct that affords emergency security measures in accordance with guidance from the Office of Civil Rights.

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

10.1 Provide for 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.

Observation: The NCVHS observes that conformance with HITSP standard content and message formats may require translation or mapping of communications prior to transmission. Entities may be able to conduct such translation or mapping themselves, or may need to have them performed by third party network service providers.

Recommendation 10: The NCVHS recommends that HHS support the continued development and testing of approaches for a nationwide health information network that demonstrate that mapping and translation functions performed by network service providers or other entities may be appropriate in environments where applicable agreements exist.

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.

    Observation: The NCVHS observes that a given query may result in identifying the existence of data at many sources, and it may be desirable to aggregate these data prior to responding to the inquiry. In addition, some locations may find it useful to create data repositories in support of healthcare quality, patient safety, biosurveillance, research, and other legitimate uses of health information.

Recommendation 11: The NCVHS recommends that HHS support the continued development and testing of prototypes for a nationwide health information network that that do not preclude transient or permanent storage of data as may be established by policy.

Gaps, Policy Issues, and Needed Standards

In the process of identifying high level functional requirements, NCVHS heard testimony regarding gaps, and NCVHS observed additional gaps in the functional requirements originally enumerated. NCVHS also identified policy issues, and recognized that in several areas consortia contractors and testifiers recommended standards that did not yet exist.

Observations about Gaps in Functional Requirements

The NCVHS has compiled the list of high level minimum but inclusive functional requirements needed for the initial definition of a nationwide health information network utilizing all of the resources available to it, including the consortia contractors' original specific functional requirements and comments from numerous testifiers. The contributions of all have permitted the NCVHS to fill in where it believes there may have been gaps in any one resource. The NCVHS has attempted to make the list of high level functional requirements as complete as possible, recognizing that as work continues to enable a nationwide health information network initiative there may well be gaps identified in this list. It is also recognized that there are high level functional requirements, specific functional requirements for any given application, and then technical requirements for any deployment of functional requirements. At each level there will be further detail, but the detail should serve to enhance and not be incompatible with the minimum but inclusive functional requirements.

The NCVHS, however, also observes that in public comments there appeared to be the perception of gaps due to the fact that functional requirements are specified at a high level. The minimum but inclusive functional requirements should be broad enough to cover any scenario, but, of course, this must be tested for any specific use case.

Recommendation 12: 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 and its various exchanges between prescribers and dispensers and special signature requirements for controlled substances; medication reconciliation within a hospital as described by JCAHO and across the continuum of care; use of clinical decision support – by caregivers and individuals (especially as related to differences in data rendering); chronic care, long term care, home health care, behavioral health care, and other settings for care; reimbursement for healthcare services; clinical research; regulatory reporting; and selected services provided by public health departments.

Policy Issues

In developing the list of high level functional requirements needed for the initial definition of a nationwide health information network, the NCVHS identified a number of areas where policy issues will need to be addressed.

In many cases, these policy issues probably could be addressed at the local or community level. At this level, there would be business agreements surrounding specific policies, procedures, and technical requirements. There are, however, some policy issues that appear to be needed for the entire networking capability to be enabled.

Recommendation 13: The NCVHS recommends that HHS:

a. Identify and recommend policy for individual identification and health information location to ensure accurate matching of individuals to their health information.

b. Support the use of standards that would enable the communication of individual permissions or entity preferences concerning specific data. Such communications have been recommended by consortia contractors and testifiers as being carried out by standard metadata. While such metadata can be applied by a given entity's systems, having metadata standards and requiring conformance to the standards appears to be a matter of policy relating to cross-entity exchange of data.

c. 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. The most common example of this is between an individual and a personal health record (PHR) vendor not affiliated with a provider or health plan. Equivalent protections could be implemented through enhancements and extensions to HIPAA or through other appropriate mechanisms. With regard to privacy protections, NCVHS has previously stated that, while a HIPAA-like framework is not necessarily the most appropriate for safeguarding privacy in PHR systems, it does believe that privacy measures at least equal to those in HIPAA should apply to all PHR systems, whether or not they are managed by covered entities.

d. Should collaborate with other public and private entities to develop a public awareness campaign regarding the value of a nationwide health information network that is grounded in sound communication research about diverse target audiences, including across various locations and communities.

Needed Standards

Several functional requirements include reference to standards. Some of the standards referenced already exist, although there may be variability in conformance of how they are used or they may only provide a framework. Many standards, by their nature, change over time with new versions being necessitated by new information requirements. New standards versions must be accommodated.

It is observed that some testifiers urged adoption of standards that were system platform independent to the extent possible. For example, a standard set of message exchange protocols such as CORBA, Web Services, SMTP (e-mail) should be able to be composed into industry specific standards, such as HL7 V3. There were also gaps identified in standards specific to health information exchange.

Recommendation 14: The NCVHS recommends that HHS support the development and adoption of standards for the following, in the context of multiple additional use cases:

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

Recommendations for Next Steps

In conclusion, the NCVHS recognizes that describing high level minimum but inclusive functional requirements needed for the initial definition of a nationwide health information network implies that there is considerable more work to support the exchange of health information in a secure and protected manner. The NCVHS makes the following recommendations for next steps with respect to the functional requirements:

Recommendation 15: The NCVHS recommends that HHS support further work to:

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 nationwide health information network

b. Evaluate the definitions of the original Functional Categories and consider refinements based on industry usage.

c. Utilize more detailed statements of functionality to illustrate specific use cases and business needs.

Appendices

See following.

Appendix A: NCVHS Work Group on NHIN

Appendix B: List of Testifiers

Appendix C: ONC Proposed Functional Requirements Categories, Version 3, April 16, 2006

Functional Categories

Audit and Logging – Functionality to support the recording of transactions and capability to review such recordings. For example, the functionality to support the identification and monitoring of activities within an application or system.

Authentication – The ability to uniquely identify and validate (to a reasonable degree) the identity of an entity. These requirements are applicable to systems, services, and organizational actors.

Authorization – The ability to determine and grant access to systems, services and data based on prescribed parameters (instantiated authorization/access policies). For example, the process of granting authority or delegation to specified actors.

Confidentiality – The ability to ensure that data are not disclosed (e.g., viewed, obtained or made known) to unauthorized individuals per organizational policies. Functionality to provide privacy, de-identification, anonymization and re-linking would be included in the confidentiality category.

Credentialing – The process of validating or confirming the qualifications of licensed professionals, e.g., clinical provider. These functional requirements are distinct from authentication and authorization.

Data Access and Update –The ability to retrieve, view, and modify data, within prescribed policies.

Data Content – There may exist requirements on data that constrain the context and use of data exchanged within the Nationwide Health Information Network. While many data requirements may be deferred to review of specifications or standards, there may be some high level data constraints that should be included within the Data Content functional category (e.g., requirement for structured or unstructured text).

Data Filtering – The functional requirements to support identifying and/or qualifying data that needs to be transmitted.

Data Mapping/Translation – The functional requirements to support reformatting or expressing data in different terms. These requirements may relate to terminology and/or message structure.

Data Quality/Data Integrity – The functional requirements to ensure data is correct and complete, including the ability to verify that data were transferred.

Data Rendering – The ability to present data.

Data Retrieval (Pull) – The functional requirements to support the request/retrieval of data.

Data Routing – The ability to identify a receiving system and ensure delivery of data.

Data Source – The functional requirements to support the identification of the data/information point of origin.

Data Transmission (Push) – The functional requirements to support the unsolicited sending of data.

Data Usage – There may exist requirements on data that constrain the context and use of data exchanged within the Nationwide Health Information Network. While many data requirements may be deferred to review of specifications or standards, there may be some high level data constraints that should be included within the Data Usage functional category.

Identity/Information Correlation – The ability to map information or entities with other entities (e.g., individuals or organizations, or necessarily a named system or network user). For example, correlating clinical information to the system or network-known identity of a patient where the patient. .

Persistent Data Storage – The ability of a system to function as a data repository.

Record Location – The ability to determine the location of data.

Transient Data – The ability of a systems to function as a data repository for a given entity for a given period of time or purpose.

Non-Functional Categories

Below is a proposed list of categories that include system qualities or "non-functional" requirements. As noted above, the expectation is that categories of non-functional requirements will only be designated where the property has a substantial impact on the architecture and capabilities of the Nationwide Health Information Network or a use case.

Accuracy – a measure of the application service quality - from the customer's perspective, the precision with which responses are provided to customer inquiries.

Business Rules – Policy driven dynamic requirements that may change during the operation of the system, requiring that the system adapt to the change without major rework.

Performance – a measure of the degree to which an entity satisfies its intended purpose.

Robustness – a measure of the ability of system to adjust to unanticipated conditions (i.e., the ability of a system to adjust to unanticipated conditions without losing its endurance and level of quality).

Scalability – a measure of the ability of system to adjust or extend to changing demands (user load, data load).

Appendix D: High Level Minimum but Inclusive Functional Requirements for Entities to Participate in a Nationwide Health Information Network, Sorted by ONC Functional Category

Audit and Logging	• Enable entities and systems to update, correct, and amend health information in accordance with HIPAA requirements and internal policies. • Ensure that all parties to the physical 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 (e.g., as may provided by HITSP standards). • 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. • 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. • Retain logs for period of time determined by law, accrediting agencies, marketplace, and entities. • Protect audit data from unauthorized access/modification. • Generate evidence to support incident management (investigations) and response processes (corrective action). • Conduct regular risk assessments.
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. • Enable an entity to register (provide authorization and establish authentication processes for) 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. • Protect authentication credentials during transmission. • Provide mechanisms for non-repudiation when policy would require such service.
Authorization	• Utilize a certification process with which any entity's health information users (systems, software tools, and individuals) must conform for exchange of data within a nationwide health information network. • 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. • Utilize HITSP standard authorization codes to convey permissions/authorizations to share data. • Enable an entity to de-identify and aggregate data, for research or

	other purposes, upon request.
Confidentiality	• Enable entities and/or users to provide permissions, authorizations, and/or restrictions to share location information/data. • Enable changes to be made in permissions, authorizations, and restrictions as requested by applicable entity and/or user. • Allow access to location of information and/or data based only on permission/authorization status or emergency access as defined by law. • Enable participants in a nationwide health information networ*k* 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).
Configuration	• Certification of entities connecting with a nationwide health information network should describe the level of participation for which an entity's information systems are capable. For example, a physician's office EHR system may only be available during specified hours to send and receive data; another entity may only be able to exchange certain types of data electronically. • The process of certifying entities to exchange data within a nationwide health information network should entail testing of capabilities; and there should be an ongoing systematic evaluation of continued conformance with the certification requirements.
Credentialing	*See Terms page 9 and Authentication*
Data Access and Update	• Provide for dynamic data access (i.e., time-sensitive request/ response interactions to specific target systems; e.g., query of immunization registry) within a nationwide health information network. • Support consistent methodology for granting and tracking access in applicable emergency situations.
Data Content	• Support content (vocabulary and code sets) and application protocols (message formats) used for the exchange of information within a nationwide health information network that conform to HITSP interoperability specifications.
Data Filtering	• Enable data filtering to allow for subscription and un-subscription to specified or all available future clinical events data.
Data Mapping/Translation	• Provide for mapping between versions of a standard and multiple standards, mapping terminologies and code sets, and supporting Section 508 compliance.
Data Quality/Data Integrity	• Provide information back to the requestor if identity, location information, and/or data could not be determined and/or provided. • Verify the integrity of data transmission. • Support the ability to include an error message service that notifies the requestor if authentication or authorization is not verified. • Provide the ability to send/receive/retransmit acknowledgment of data requests or data content retransmissions.
Data Rendering	• Support display, entry, and retrieval of data in multiple ways as determined by the needs of the recipient.
Data Retrieval (Pull)	• Provide notification concerning location of information, pointers to the locations, or the data itself to the requestor depending on the

	structure of the network used and agreements in place. (Also applies to Data Transmission [Push]). • Enable standard information metadata (e.g., UML, XSD, and/or HITSP-specified) to be included in data retrieval or delivery of messages in order to convey, for example, sensitivity restrictions, individual permissions, and entity preferences.
Data Routing	• 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.
Data Source	• Identify the source of any externally-provided data.
Data Transmission (Push)	• Support the ability to move or copy 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. • 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.
Data Usage	• Enable entities to acquire data to monitor a previously detected event, generate alerts/notifications, or perform similar functions.
Identity/Information Correlation	• Uniquely identify an individual through matching on various identifiers, such as last name, middle name, first name, date of birth, gender, etc. • Utilize a process to resolve identity ambiguities, consistent with applicable tolerance levels for errors.
Persistent 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.
Record Location	• Utilize a (HITSP standard) person identity/information correlation process to uniquely identify an individual. • Provide functionality that will locate where health information exists for identified individuals. • Utilize a standard, unique organizational identifier to locate entities holding a specific individual's information.
Transient Data	• Support the ability to hold and aggregate appropriate error messages or data based on an entity's query.

1132

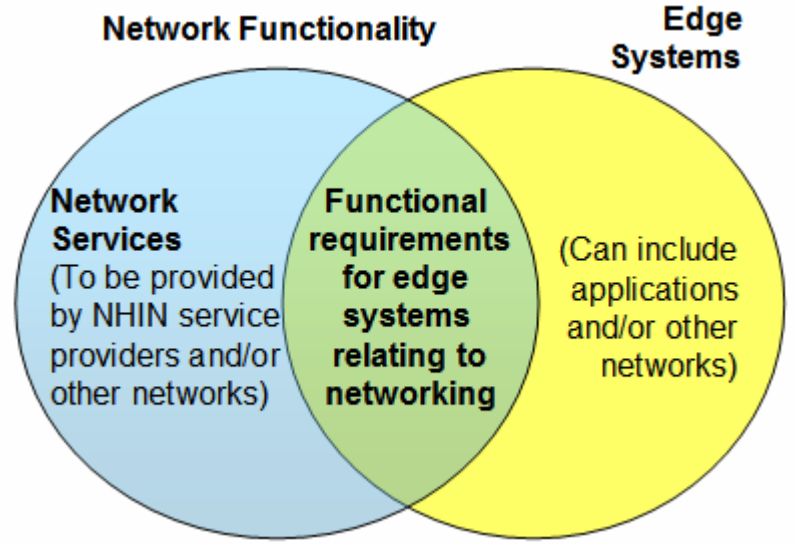
Appendix E: Analysis of Original 977 Functional Requirements

The set of original 977 functional requirements enumerated by the consortia contractors is provided in the **attached spreadsheet**.

The original 977 functional requirements were identified by the consortia contractors as those that may be performed by entities whose primary purpose was to provide networking services, identified initially by ONC as "core systems," and those that may be performed by various other entities, identified initially by ONC as "edge systems." Edge systems may be EHRs in care delivery organizations, terminology servers provided by vendor systems, etc. Some edge systems provide application support exclusively and others provide both application and networking support.

Because the terms "core" and "edge" did not convey the notion that "core" was comprised of many entities and that "edge" systems could also provide networking functionality, these terms were first refined as illustrated in the Venn diagram below.

Interim Categorization of Functional Requirements for a Nationwide Health Information Network



Each of the 977 functional requirements was then labeled as pertaining to one of the three locations, using the following definitions:

Network functionality (N) may be provided by network service providers and/or other networks.

Functional requirements for edge systems relating to networking (E). These functional requirements may at different times and different locations be performed by different types of entities.

Functions that apply eXclusively to an edge system (X) are those where an application at a specific location interacts with the information and applies it in a useful and appropriate manner. NCVHS has identified these within the analysis of the complete set of detailed functions as those that apply exclusively to edge functionality. NCVHS has not brought these “X” functions forward as part of the minimum but inclusive networking functions.

In addition to analyzing where a functionality may occur, the NCVHS considered how closely one functional requirement resembled one or more other requirements, and annotated these relationships.

Appendix F: Derivation of Interim Working Set of Functional Requirements

The set of interim functional requirements derived by the NCVHS is provided in the **attached spreadsheet**.

While the NCVHS analysis process began with a review of 977 functional requirements initially identified by the ONC consortia contractors, the contractors and other testifiers to the NCVHS helped frame the consolidation of the functional requirements into the high level view ultimately presented in the body of this report. However, an interim step was used to reach the high level minimum but inclusive functional requirements. The process of deriving this working set included the consolidation of functionalities that closely resembled one another.

The initial location categorization of Network Functionality and Networking Functions Performed by Edge Systems was retained. However, within the functional requirements for edge systems relating to networking, two categorizations were identified: Where the function related generically to locations and content, it was categorized as GENERAL EDGE. Where the function was specific to a location or content, it was categorized as SPECIFIC EDGE.

In addition to consolidating the functional requirements that closely resembled one another, gaps identified by NCVHS and its testifiers were added.

Appendix G. High Level Minimum but Inclusive Functional Requirements for Entities to Participate in a Nationwide Health Information Network Mapped to Interim Working Set of Functional Requirements

Appendix H. Summary of Patient Matching Testimony

Appendix I: Differences in Design of Services (Architectural Variations)

To facilitate the inclusion of differences in design of services in the high level minimum but inclusive functional requirements needed for the initial definition of a nationwide health information network, ONC provided the information flows in the **attached presentation** material.