

## Summary of the NHIN Prototype Architecture Contracts

A Report for the Office of the National Coordinator for Health IT

31 May 2007

Engagement: 221630040

## Table of Contents

<b>1.0</b>	<b>Introduction .....</b>	<b>2</b>
1.1	Executive Summary .....	2
1.2	Road Map to This Report.....	6
<b>2.0</b>	<b>Overview of NHIN Prototype Architecture Projects .....</b>	<b>9</b>
2.1	Prototype Architecture Requirements and Conceptual Overview.....	9
2.2	Participants and Approaches.....	11
2.2.1	Accenture Prototype Architecture.....	12
2.2.2	CSC-Connecting for Health Prototype Architecture.....	14
2.2.3	IBM Prototype Architecture.....	17
2.2.4	Northrop Grumman Prototype Architecture .....	19
2.3	Summary of Accomplishments .....	21
<b>3.0</b>	<b>An Overview of the NHIN .....</b>	<b>24</b>
3.1	Benefits.....	24
3.2	Constituents of the NHIN .....	24
3.2.1	The Health Information Exchange .....	24
3.2.2	The NHIN Health Information Exchange .....	25
3.2.3	Specialized NHIN Participants.....	27
3.2.4	Health Information Service Providers (HSPs) .....	27
3.3	Related ONC Initiatives .....	27
<b>4.0</b>	<b>NHIN Operational Services.....</b>	<b>32</b>
4.1	Operational Services .....	32
4.2	The Role of Interoperability in Supporting Operational Services .....	33
<b>5.0</b>	<b>Interchange Capabilities.....</b>	<b>36</b>
5.1	Operational Services vs. Interchange Capabilities .....	36
5.2	Annex Format .....	38
5.2.1	Foundational Transaction Packages .....	41
5.2.2	NHIE Logical Registries.....	41
5.3	Common Transaction Features .....	42
5.3.1	Audit Logging.....	42
5.3.2	Authentication (Person).....	42
5.3.3	Authentication (System) .....	43
5.3.4	Data Integrity Checking .....	43
5.3.5	Error Handling .....	43
5.3.6	HIPAA De-Identification.....	43
5.3.7	Holding Messages .....	43
5.3.8	Non-repudiation .....	43

5.3.9	Patient Summary Record Support.....	43
5.3.10	Pseudonymize and Re-Identify.....	44
5.3.11	Secure Transport.....	44
5.3.12	Transmit Disambiguated Identities .....	44
5.4	Ensuring Authorization.....	45
5.5	Concluding Comments.....	46
<b>Annexes</b>	.....	<b>48</b>
Annex 1.	Arbitrate Identity.....	52
Annex 2.	Identify Subject .....	56
Annex 3.	Locate Records.....	60
Annex 4.	Maintain Consumer Data Sharing Permissions .....	64
Annex 5.	Maintain Registries of NHIN-Participating Systems and Organizations.....	68
Annex 6.	Manage Data Selection Parameters for Secondary Use .....	71
Annex 7.	Provide Consumer Access to Access and Disclosure Logs .....	75
Annex 8.	Provide Data to Secondary Users.....	79
Annex 9.	Pseudonymize and Re-Identify Data .....	83
Annex 10.	Publish PHR Location .....	87
Annex 11.	Retrieve Data .....	91
Annex 12.	Route Consumer Request to Correct Data .....	95
Annex 13.	Route Data.....	99
Annex 14.	Route Data Based on Consumer-Specified Preferences.....	102
<b>Appendix 1: Glossary</b>	.....	<b>107</b>

## List of Tables

Table 1.	AHIC 2006 Use Cases, Select Functional Requirements.....	10
Table 2.	Accenture Participants.....	12
Table 3.	CSC Participants .....	15
Table 4.	IBM Participants .....	17
Table 5.	Northrop Grumman Participants.....	19
Table 6.	NHIN Core Services and Capabilities.....	33
Table 7.	Treatment of Operational Services in This Document.....	36
Table 8.	Operational Services, Interchange Capabilities and Common Features.....	36
Table 9.	NHIE Logical Registries.....	41
Table 10.	Annex Overview .....	48

**List of Figures**

Figure 1.	Cyclic Steps to Achieving the NHIN .....	5
Figure 2.	Road Map to This Report .....	7
Figure 3.	Accenture Approach .....	13
Figure 4.	CSC Approach.....	16
Figure 5.	IBM Approach.....	19
Figure 6.	Northrop Grumman Approach .....	20
Figure 7.	A Health Information Exchange.....	25
Figure 8.	An NHIE Supporting Another HIE.....	26
Figure 9.	The Relationship of Architecture to Other NHIN Initiatives.....	28
Figure 10.	NHIN Standard Interfaces .....	34
Figure 11.	NHIE Value-Added Services: Adapted Interfaces .....	34
Figure 12.	An Example of an Annex Diagram .....	39
Figure 13.	Annotated Example of Annex Diagram .....	40

## ***Authors' Note***

We are pleased to have been invited to review the NHIN prototype architecture project outcomes and to work with ONC to synthesize those learnings into this report. This is an exciting time for the U.S. healthcare market, and we hope that this report captures the progress enabled by these projects and the ensuing discussions and activities of ONC and the broad community of those supporting the NHIN.

First, we would like to thank Dr. John Loonsk, Director for Interoperability and Standards at the ONC, for his ongoing input, advice and collaboration during this process.

All four contractors were very generous with their time and insights, and we are grateful to them for their ongoing contributions. A report such as this can never capture exactly the diverse positions of four talented groups. However, even where there were differences, the contributions of all were based on a deep understanding of the issues and were motivated by a commitment to the success of the NHIN. We particularly thank:

- From Accenture: Brian Kelly, Asad Khan, Martin Renwick and Garret Wu
- From CSC/Connecting for Health: Greg DeBor, Carol Diamond, Vinod Muralidhar, Dr. Marc Overhage, Clay Shirky and Dr. Robert Wah
- From IBM: Houtan Aghili, Richard Steen and Ginny Wagner
- From Northrop Grumman: Wendell Ocasio and Robert (Rim) Cothren

We would also like to thank Ken Gebhart from BearingPoint for reviewing this report in light of its efforts in support of the most-recent round of use case development.

Finally, we must note that the concepts and terminology contained in this report are in many ways still dynamic and evolving. We have attempted to capture a snapshot of a moving target and, as a result, we may have traded off some details in an effort to produce this report in a time frame where it is still relevant. We do not presume to have produced a final or definitive summary of the NHIN, but we have synthesized our best understanding of its current state, advances and remaining issues, in the hopes that the NHIN prototype project results will be more fully realized and leveraged in the ongoing evolution of the NHIN.

Wes Rishel, Virginia Riehl and Cathleen Blanton

Gartner, Inc.



■ ■ ■ ■ **Executive Summary**

## 1.0 Introduction

### 1.1 Executive Summary

In describing progress in Healthcare IT, Secretary Michael Leavitt wrote<sup>1</sup>:

Today, evidence that use of secure, standards-based, electronic health records can improve patient care and increase administrative efficiency is overwhelming. This use of interoperable health information technology (IT) will benefit individuals and the health-care system as a whole in profound ways.

A cornerstone in the plan for interoperable health information technology is the progress that has been made toward enabling the creation of a Nationwide Health Information Network (NHIN), a “network of networks” that will securely connect consumers, providers and others who have, or use, health-related data and services, while protecting the confidentiality of health information. The NHIN will not include a national data store or centralized systems at the national level. Instead, the NHIN will use shared architecture (services, standards and requirements), processes and procedures to interconnect health information exchanges and the users they support.

Creating the NHIN is a substantial challenge. There are issues of scale, complexity, protecting privacy, working with existing IT systems and ensuring that the NHIN approach does not unnecessarily hamper innovation in healthcare IT systems. Accordingly, in November 2005, the Office of the National Coordinator for Health IT (ONC) awarded four contracts for developing prototype architectures for an NHIN to Accenture, Computer Sciences Corporation, IBM and Northrop Grumman. Each contractor was asked to develop a prototype architecture for the NHIN and to interconnect three communities as a demonstration of the architecture.

#### *Initial Successes*

These contracts each validated important basic principles that underlie the current approach to the NHIN. These principles include:

- The possibility of operating the NHIN as a network of networks without a central database or services
- The criticality of common standards for developing the NHIN, particularly in the way that component exchanges interact with each other
- Synergies and important capabilities can be achieved by supporting consumers and healthcare providers on the same infrastructure
- Consumer controls can be implemented to manage how a consumer’s information is shared on the network
- There can be benefits from an evolutionary approach that does not dictate wholesale replacement or modification of existing healthcare information systems

---

<sup>1</sup>Leavitt, “U.S. Department of Health and Human Services Health Information Technology Initiative Major Accomplishments: 2004–2006”, <http://www.hhs.gov/healthit/news/Accomplishments2006.pdf>, Jan 2007, p.6.

The substantive commonalities of the approaches can be coalesced into the go-forward approach that supports the next steps in building an NHIN that supports the U.S. Health IT Agenda.

The contractors delivered reports throughout 2006 describing functional requirements of the NHIN, security models, areas for needed standards, an overall architecture, and business models. The prototype architecture projects culminated with live demonstrations at the NHIN Prototype Architecture Project Third NHIN Stakeholder Forum on 25–26 January 2007.

This report is a synthesis of their approaches as a basis for the next steps in creating the NHIN.

### *Architecture*

The term “architecture” is used in a wide variety of contexts to describe an orderly arrangement of parts. On a grand scale, an example of an architecture is city planning—that is, ensuring that various “parts” (roads, sewage, housing developments and recreational facilities) work together to meet growth and social requirements.

In the architecture of a network, the “parts” are generally subsystems and interfaces.<sup>1</sup> For example, in the architecture of the Internet, the subsystems are clients and servers. The Internet architecture is similar to “city planning” in that it attempts to “govern best by governing least.” By defining a few general subsystems and focusing primarily on the interfaces, it balances the conflicting goals of coordinating disparate elements and providing flexibility for innovation.

The “subsystems” of the NHIN actually will be the systems of a variety of stakeholder organizations. At any point in time these systems will be in different stages of their life cycles, will be built on many different technologies, and have differing views of the data they collect. A goal in enabling the NHIN is to follow the “city planning” approach, i.e., to focus on technology-neutral interfaces among these disparate systems to create a network of networks so that participation in the NHIN will not require “ripping out and replacing” existing systems.

### *NHIN Participants*

The stakeholders that participate in the NHIN will be four broad classes of organizations:

- Care delivery organizations (CDOs) that use electronic health records (EHRs).
- Consumer organizations that operate personal health records (PHRs) and other consumer applications.
- Health information exchanges (HIEs): multi-stakeholder entities that enable the movement of health-related data within state, regional or non-jurisdictional participant groups.
- Specialized participants: organizations that operate for specific purposes including, but not limited to, secondary users of data such as public health, research and quality assessment. The specialized nature of these organizations means that they may require only a subset of the shared architecture (standards, services and requirements), processes and procedures used by the other participants.

Many of these organizations will have their own networks. The NHIN is not intended to supplant these networks. They will continue to handle the bulk of day-to-day transactions in providing and

---

<sup>1</sup> The word “interface” has a variety of meanings, including some very specific but different meanings in engineering. This report uses the term in a general sense: “...a means of interaction between two devices or systems that handle data.”

measuring healthcare. This is why the NHIN will be a “network of networks,” built over the Internet. It provides the interconnection so that these networks can support additional information exchange beyond their own bounds.

To participate in the NHIN, an organization will be required to use a shared architecture, adhere to adopted standards and provide certain core services. Not all HIEs may choose to do so. An NHIN health information exchange (NHIE) will be one that implements the NHIN architecture (services, standards and requirements), processes and procedures and participates in the NHIN Cooperative.

### *Health Information Service Providers (HSPs)*

Some organizations may lack the necessary technical or operational competencies to conform to the architecture and provide the core services. Instead, they may choose to use the services of an HSP. An HSP is a company or other organization that will support one or more NHIN participants by providing them with operational and technical health exchange services necessary to fully qualify to connect to the NHIN.

### *How a Person Will Use the NHIN*

The business, trust and technical arrangements that will enable the NHIN generally will be local and between organizations. Nonetheless, the primary users of the NHIN will be people: healthcare providers, healthcare consumers and those who use the data in the NHIN for public health, quality assessment or other purposes. These people will have several ways to take advantage of the information exchange available through the NHIN. Here are several access paths for healthcare providers.

- Providers may use features of the electronic health record (EHR) systems of their own practice or hospital to connect to an HIE, and the HIE, in turn, will support information exchange with other EHRs or PHRs on that HIE or on other HIEs through the NHIN.
- They may not have an EHR, so they may use the Web to access a portal operated by the HIE to access information.

The paths to the NHIN are similar for healthcare consumers.

- They may use features of a PHR that they designate as the repository of their personal health record, and that PHR may be connected to an HIE which, in turn, will provide a connection to the NHIN.
- They may use features of a multi-regional PHR that will participate directly in the NHIN.
- If they do not have access to a PHR, they may achieve some limited functionality by using the services of an HIE through its portal.

### *Relationship to Policy*

The NHIN architecture is strongly related to policy. Policy informs architecture by identifying specific requirements that must be met by systems implemented according to the architecture. Architecture informs policy and policy development by enabling policymakers with approaches and solutions. In the U.S. today, however, there is substantial heterogeneity among the laws and regulations of the states, and many policies were developed during a time when information sharing was primarily done on paper or by fax. The ONC has several initiatives under way to create more consensus on policy issues and to update policies based on the challenges and limitations of electronic information exchange at national, state and local levels. Because this is a sensitive area, and because the potential impact of policy options is not always understood,

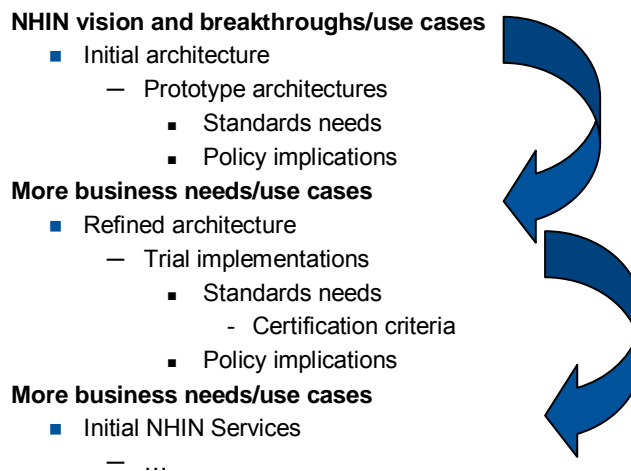
the relationship between architecture and policymaking is bidirectional. The architecture must have the flexibility to accommodate changes in policy that will be identified in the future. At the same time, the industry must get enough experience with the architecture to realistically predict the costs of various approaches. Approaching policy and architecture issues in parallel is the only viable approach to sorting out complex, sensitive issues for large-scale systems.

### *Cyclic, Step-Wise Approach*

Just as there is a need to approach policy and architecture in parallel, there is a similar need to approach architecture and standards and certification of participating systems in parallel. Accordingly, the NHIN Prototype Architecture Project is part of the first of a series of cyclic steps toward achieving the NHIN as shown in Figure 1. Repeating this cycle allows those working on the various aspects of the NHIN to work in group and focus on achieving manageable increments of progress.

The second cyclic step will include a set of projects known as the NHIN Trial Implementations.

**Figure 1. Cyclic Steps to Achieving the NHIN**



### *The Synthesized Approach*

The general approach of the contractors had much in common. Specifics varied to the degree that was expected from four independent efforts. Each contractor considered the NHIN as a set of distributed HIEs that work together to become the NHIN. They each identified specific functions that must be provided by the HIEs, including:

- Supporting secure operation in all activities related to the NHIN
- Protecting the confidentiality of personally identifiable health information as it is used by those who participate in the NHIN
- Reconciling patient and provider identities without creating national indices of patients
- Providing a local registry which may be used, when authorizations permit, to find health information about patients
- Supporting the transfer of information from one provider or care delivery organization to another in support of collaborative care
- Supporting secondary uses of data while protecting the identity of patients to the degree required by law and public policy

Through the work of the Office of the National Coordinator, the National Committee on Vital and Health Statistics (NCVHS) and Gartner, the specifications in support of these functions have been consolidated into 24 specific operational services. These services are listed in Section 4.0. Many of these business or operational services imply interfaces among information systems. Fourteen of such implied interfaces are also identified described in Section 5.0 and the Annexes of this report.

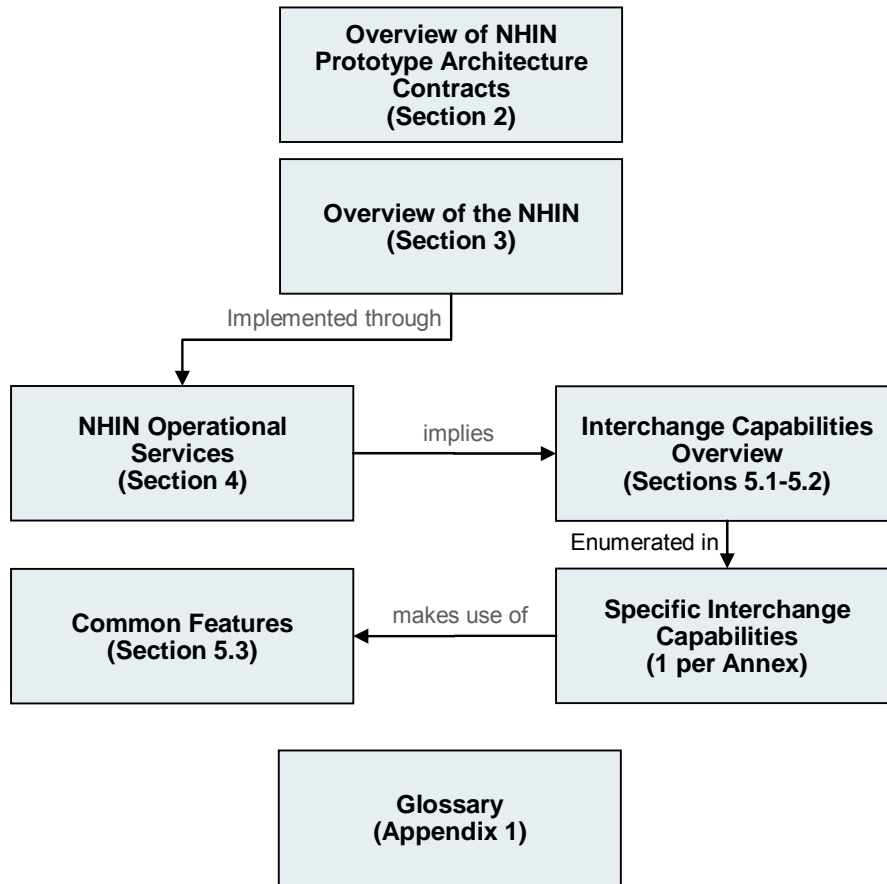
It is expected that the identified services and interfaces will be addressed through ongoing work in several projects during and following 2007, including a series of trial NHIN implementations by HIEs that together will constitute an initial NHIN cooperative.

## **1.2 Road Map to This Report**

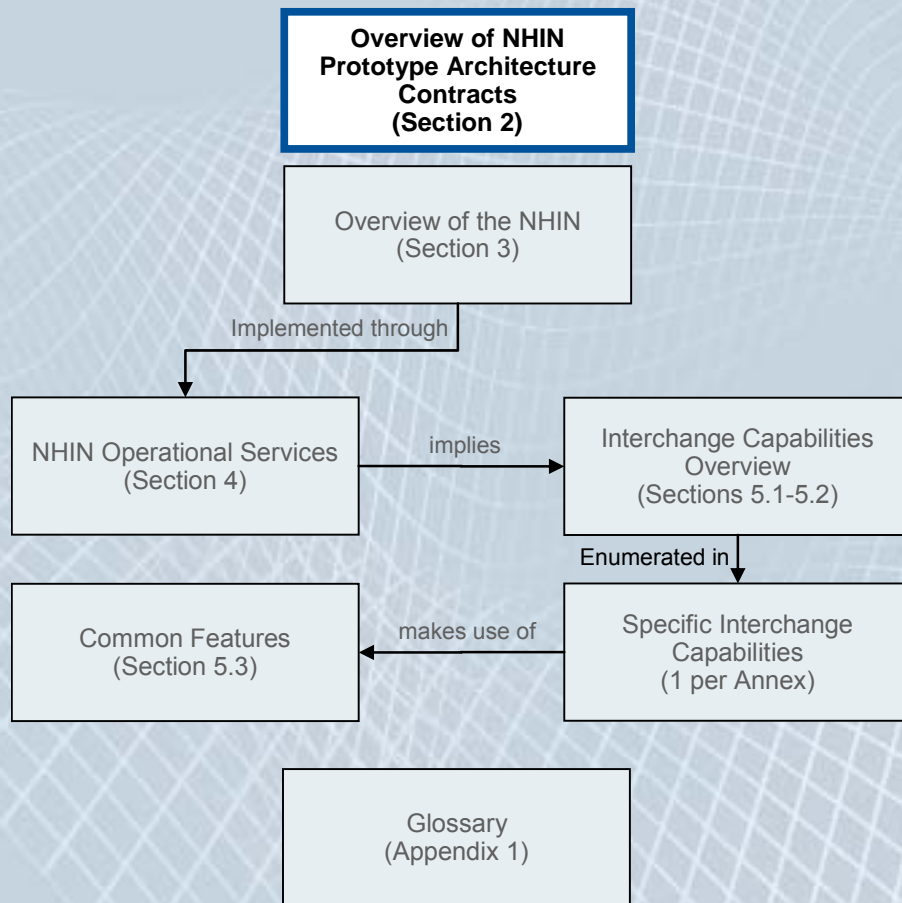
This report includes an overview of the architectural deliverables of the contractors in a format that emphasizes the common features that serve as building blocks for future NHIN efforts. Those building blocks are described first as the operational services of the NHIEs. Delivering many of the operational services requires interfaces among the NHIEs or between an NHIE and its participants. The information interchange is accomplished through those interfaces, which are categorized into interchange capabilities. Figure 2 shows how these topics are organized in this report.

Although Section 5 and the Annexes have some of the characteristics of technical specifications, they are at a high level of abstraction. This approach serves to support diverse approaches going forward. The detailed specifications required for the NHIN will be developed in the go-forward activities that support building the NHIN.

**Figure 2. Road Map to This Report**



## Overview of NHIN Prototype Architecture Projects



## 2.0 Overview of NHIN Prototype Architecture Projects

As described in the Executive Summary, the NHIN prototype architecture contracts are a significant contribution to the overall NHIN evolution. The lessons learned through these prototypes will, with other concurrent efforts, feed the design and standards development processes related to the NHIN Trial Implementations. The prototyped designs of the contractors will inform the standards development process and the NHIN trial implementations. This section describes the participant consortia and their conceptual approaches as context for understanding what was accomplished.

### 2.1 Prototype Architecture Requirements and Conceptual Overview

In November 2005, HHS Secretary Michael Leavitt announced that the first NHIN prototype contracts were awarded to four consortia that would demonstrate exchanging health information based on needs to connect health records based on the requirements of the first three use cases.

Each of these consortia developed and demonstrated a prototype architecture for an NHIN, descriptions of that architecture and software that validated that the architecture could indeed function. Each prototype was ultimately required to:

- Interconnect several communities that consist of real healthcare organizations<sup>3</sup>
- Show support for consumers and healthcare providers
- Validate that the NHIN can operate as a “network of networks”
- Validate that these networks can be interconnected in a peer-to-peer manner without substantial centralized or national infrastructure
- Interconnect with systems and networks that were built using a variety of heterogeneous technologies
- Demonstrate their architecture in a manner that would be meaningful to clinicians and consumers
- Show functionality based on health information exchange and three of the four use cases recommended to the Secretary of HHS by the AHIC in May 2006 as shown in Table 1
- Locate patients by demographic characteristics without a unique national identifier
- Maintain security and confidentiality of patient data
- Meet additional needs of the use cases such as allowing patients to manage access permissions for their personal health records

---

<sup>3</sup> There was not, however, a requirement to share actual protected health information of real patients for these demonstrations of prototypes.

**Table 1. AHIC 2006 Use Cases, Select Functional Requirements.**

Use Case	Select Functional Requirements
<b>EHR/Lab Use Case</b>	<ul style="list-style-type: none"> <li>■ Allow ordering and authorized non-ordering physicians to receive current lab results in an EHR</li> <li>■ Allow ordering and authorized non-ordering physicians to access historical lab results</li> </ul>
<b>Consumer Empowerment Use Case</b>	<ul style="list-style-type: none"> <li>■ Support the delivery of medication information and medication history to a consumer's PHR</li> <li>■ Allow consumers to establish and manage permissions for accessing their personal health record</li> <li>■ Secure data according to those permissions</li> <li>■ Support the delivery of registration data to EHRs</li> <li>■ Support the delivery of medication data to PHRs and access to this data by physicians</li> </ul>
<b>Biosurveillance Use Case</b>	<ul style="list-style-type: none"> <li>■ Provide standardized, pseudonymized<sup>4</sup> health information to public health organizations to support public health needs</li> </ul>

Each of the contractors was able to demonstrate NHIN connectivity in support of the requirements stated above by implementing the technical approaches described in this section of this report. For the most part, the prototype architectures validated the requirements stated above. Individual variances are noted below.

Each approach was based on the principle of the “narrow waist” or “middle-out” design<sup>5, 6</sup>. The apparent paradox of this approach is that the best way to support heterogeneity and evolutionary innovation across a wide variety of participants in a large network is to enforce homogeneity for a small, well-chosen set of interfaces at the center. In the NHIN, the NHIEs will serve as the “funnels” that, at the wide end, assist the widest variety of healthcare IT systems to interconnect and, at the narrow end, connect among themselves in tightly standardized ways.

It must be noted that the standard interfaces at the narrow end of the funnels are, for the most part, suitable for much broader use. Indeed, to the extent that the developers of healthcare IT systems build these standards into their products, it will become much simpler and less costly to integrate systems and compare data accumulated by those systems. However, even if all the standards were fully developed today and all developers had had the time to adapt their systems to the standards, it would still be many years before the new and updated healthcare IT systems would be able to replace the legacy systems in place today. The ability of the NHIEs to bridge the gaps to in-place systems is a critical factor in achieving interoperability among healthcare IT systems. A common analogy to the process of rolling out the NHIN is to describe it as “changing the tires on a moving car.”

<sup>4</sup> Derived from “pseudo-anonymize,” this means modifying personal health information such that (a) the identity of the subject is not immediately apparent, (b) the information content fits the needs of the use case and (c) it is possible for the agent that modified the data, or its designee, to restore the identity information upon authorized request.

<sup>5</sup> David D. Clark, “[Interoperation, Open Interfaces, and Protocol Architecture](#)” The Unpredictable Certainty: White Papers, National Academies Press (1997), p 133.

<sup>6</sup> See also the work of John C. Doyle on mesoscale architecture, e.g., Lego Spanning Layer (Hourglass) Presentation at <http://www.cds.caltech.edu/~doyle/CmplxNets/LegoPics.pdf>.

All four consortia addressed at least these capabilities in their architectures:

- Support for PHRs and EHRs
- Patient identification by demographics, without a national ID
- Provider identification
- Location and retrieval of a patient's health information
- Pseudonymization and re-identification of protected health information
- Support for translating coded data into standard coding systems and back
- Support for mapping messages between non-standard formats and current or new standards
- Support for routine messages to a destination at times across NHIEs
- Secure and reliable message delivery
- Auditing
- Authentication and authorization
- Permissions management

As was expected from four separate design efforts, there were individual differences in the names that the firms gave to modules of their systems that support the NHIN functions. Furthermore, in some cases they differed in how the functions were factored together. After giving an overview description of the individual approaches, the rest of this report will describe a synthesis that serves as a high-level basis for going-forward NHIN work.

## 2.2 Participants and Approaches

The NHIN prototype contract awards were made to four consortia. Each was led by a systems integrator that coordinated efforts with healthcare market organizations—both HIEs and providers—and technology partners and vendors.

The following sections show how the different prototype architecture implementations support the conceptual architecture described in this document.

### 2.2.1 Accenture Prototype Architecture

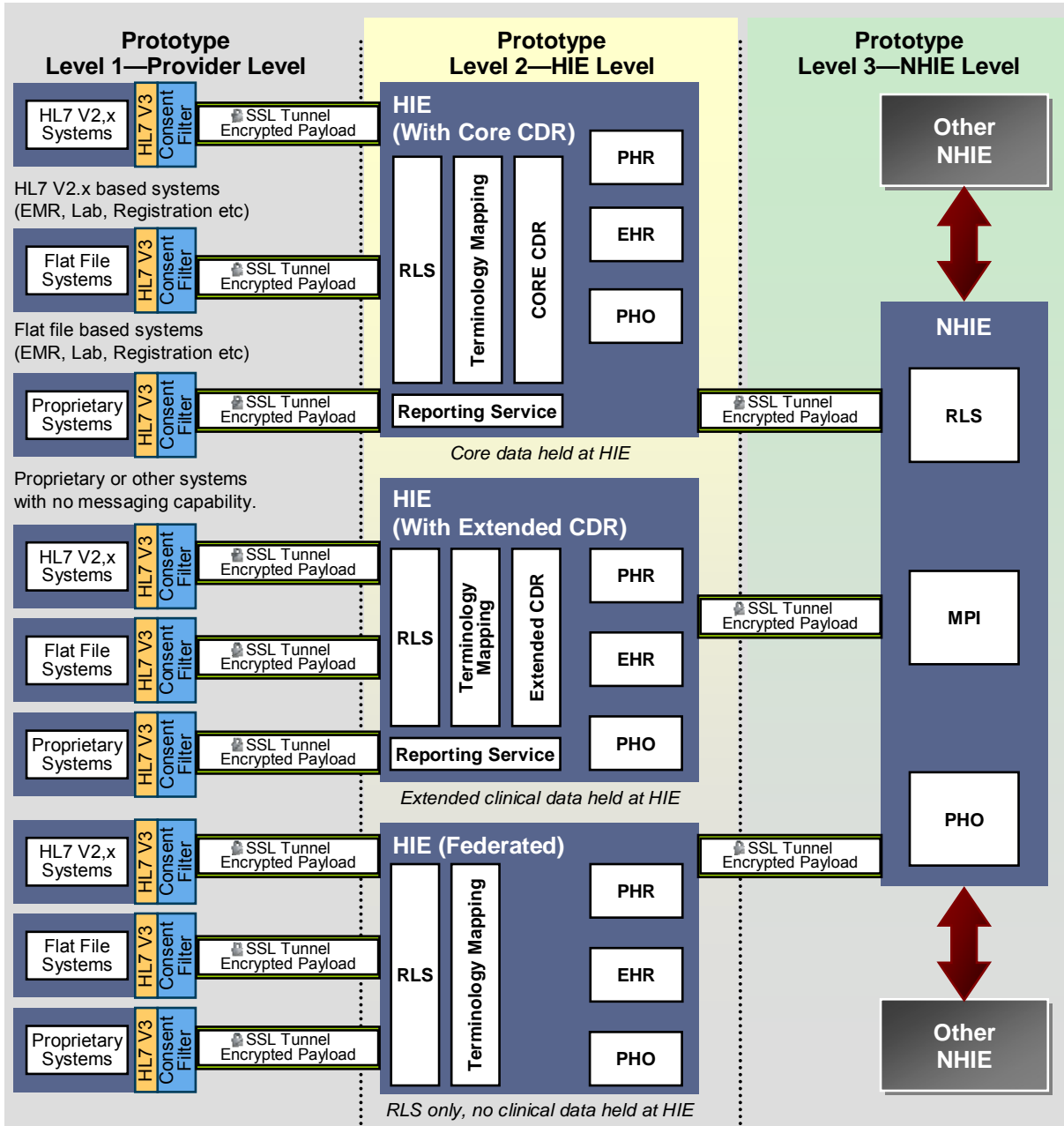
Accenture’s consortia worked with care delivery organizations in West Virginia, Tennessee and Kentucky, as shown in Table 2 below.

**Table 2. Accenture Participants**

Healthcare Market	Technology Partners and Providers
<ul style="list-style-type: none"> <li>■ West Virginia Medical Institute                             <ul style="list-style-type: none"> <li>□ New River Health Association—Beckley</li> <li>□ Cabin Creek</li> <li>□ ARH-Beckley</li> <li>□ ARH Summers County</li> <li>□ AMFM-Beckley</li> <li>□ WV University Physicians of Charleston</li> </ul> </li>   <li>■ Commonwealth of Kentucky’s Eastern Kentucky Regional Health Community                             <ul style="list-style-type: none"> <li>□ ARH-Hazard Regional Medical Center and Family Health Services</li> <li>□ University of Kentucky Clinic</li> <li>□ University of Kentucky HealthCare Chandler Medical Center</li> <li>□ Kentucky River District—Letcher County Health Dept.</li> <li>□ Kentucky River District—Perry County Health Dept.</li> </ul> </li>   <li>■ CareSpark (Tennessee)                             <ul style="list-style-type: none"> <li>□ Holston Medical Group</li> <li>□ Mountain States Health Alliance</li> <li>□ Johnston Memorial Hospital</li> <li>□ Sullivan County Regional Health Department</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>■ Core Technical Components and Partners                             <ul style="list-style-type: none"> <li>□ Cisco Systems</li> <li>□ Initiate Systems</li> <li>□ Oracle</li> <li>□ Orion</li> <li>□ Quovadx</li> <li>□ Sun Microsystems</li> </ul> </li>   <li>■ Technical Partners                             <ul style="list-style-type: none"> <li>□ Apelon</li> <li>□ AMA</li> <li>□ BEA</li> <li>□ CCSi</li> <li>□ CGI-Federal</li> <li>□ Intellithought, Lucent Glow</li> <li>□ Oakland Consulting Group</li> <li>□ Reactivity</li> <li>□ Red Hat</li> </ul> </li> </ul>

In Figure 3, Accenture illustrates how it structured its NHIN prototype implementation.

**Figure 3. Accenture Approach**



Source: Accenture

None of Accenture’s distinct healthcare markets had existing health information exchanges (HIEs) at the start of the prototype. The capabilities and infrastructure appear in the prototype architecture at three levels:

- **Level 1 (Provider Level).** At the level of the participating care organization, Accenture provided multiple data extraction mechanisms to convert local data into standard, HL7 v3 message formats. Data could be accepted from multiple sources including HL7 v2-based messaging systems, as a flat file derived from local systems, and from proprietary

systems without messaging capabilities. These messages were filtered so that only messages from patients who consented to participate in the local HIE and/or NHIN prototype were sent outside the care organization's firewall. This approach lessens the barrier of entry to care organizations because it reduces the need to alter their systems or add additional infrastructure.

- **Level 2 (HIE Level).** These HIEs had record locator services (RLS), as well as patient matching and information governance capabilities. Additionally, lab, demographic and medication data coming via HL7v3 messages were mapped from the local terms to Federal Health Architecture (FHA) vocabulary standards to facilitate secondary uses of the data. This normalization process allowed for NHIE-wide data comparisons and enhanced abilities to analyze and graph data. The architecture was specified so that the amount of data stored in the local HIE could be determined regionally. The data stored at the local HIE could be a core clinical data set, an extended clinical data set, or no clinical data at all. In the actual prototype, all three healthcare markets favored storing of a core set of clinical data. In the Accenture prototype, data could be viewed through a portal at the local HIE level with views available for the patient, providers and public health officials. The architecture supports the capability for messaging back to provider systems so that information from the NHIN can be viewed through local systems.
- **Level 3 (NHIE Level).** The level labeled NHIE contains facilities for cross-indexing patients and providers, and identifying the location of records on a patient. The components of level three that are depicted in blue were part of the Accenture prototype deliverable, whereas the items depicted in gray were not, but show how different NHIEs would interact.

In this approach, the thin NHIE layer provides cross-regional indexing mechanisms for matching patients and sending data from one local HIE to another, as well as providing mechanisms to interact with other NHIEs. Data Services are provided through the message handling services at the provider and local HIE levels, along with the record locator services and re-linking (de-pseudonymization) services. The Master Patient Index (MPI) shown at the NHIE level, along with authentication and authorization, are similar to the User and Subject Identity Management operational services. The reporting services shown in Figure 3 are for authorized secondary users—in areas such as public health, biosurveillance, and research—to access pseudonymized electronic health information.

## 2.2.2 CSC-Connecting for Health Prototype Architecture<sup>7</sup>

Table 3 lists the healthcare market and technology partners and providers that participated in the CSC NHIN prototype architecture consortium.

---

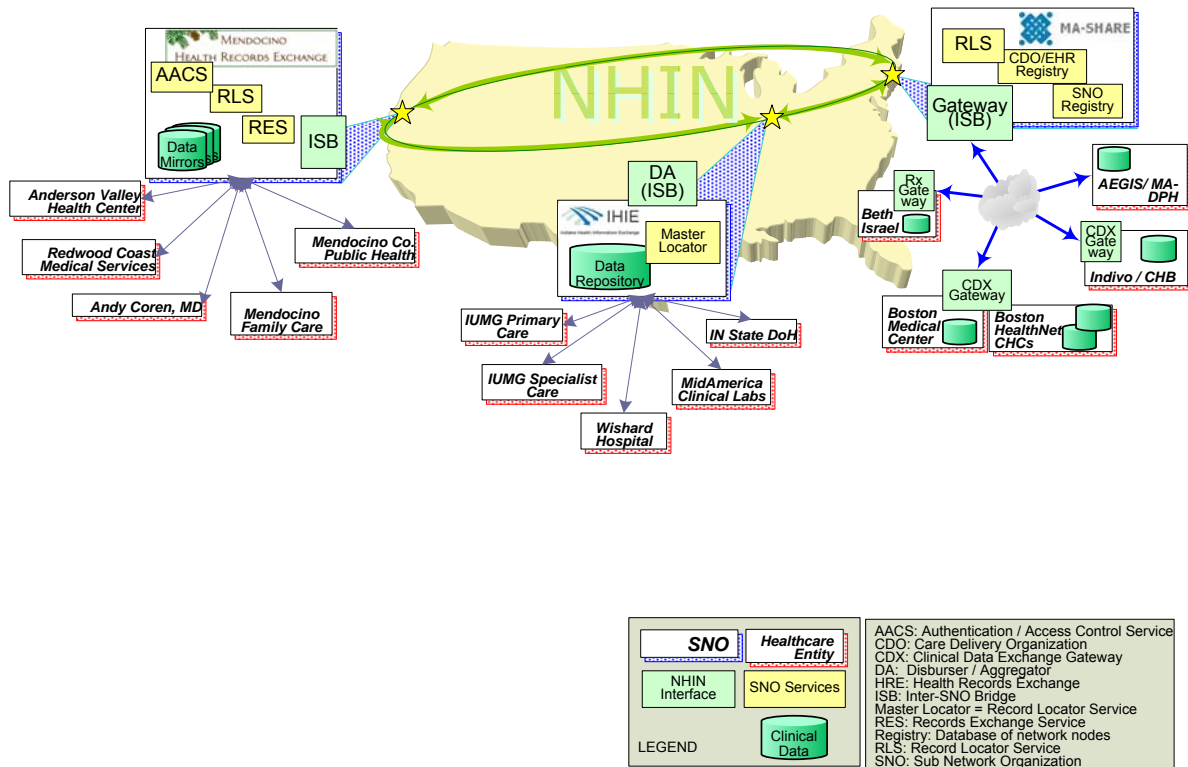
<sup>7</sup> Because of the nature of the team collaboration between CSC and Connecting for Health, CSC refers to this as the CSC-Connecting for Health Team Prototype Architecture. See [www.connectingforhealth.org](http://www.connectingforhealth.org).

**Table 3. CSC Participants**

Healthcare Market	Technology Partners and Providers
<ul style="list-style-type: none"> <li>■ Indiana Health Information Exchange (Indiana) <ul style="list-style-type: none"> <li>□ Wishard Hospital</li> <li>□ Indiana University Medical Group (IUMG) Primary Care</li> <li>□ IUMG Specialty Care</li> <li>□ Indiana Department of Health (ESSENCE)</li> <li>□ Mid America Clinical Lab</li> </ul> </li>   <li>■ MA-SHARE (Massachusetts) <ul style="list-style-type: none"> <li>□ Boston Medical Center</li> <li>□ Whittier Street Health Center</li> <li>□ South Boston CHC</li> <li>□ Beth Israel Deaconess Medical Center (BIDMC)</li> <li>□ Children’s Hospital Boston (CHB)</li> <li>□ Massachusetts Department of Public Health (AEGIS)</li> </ul> </li>   <li>■ Mendocino HRE (California) <ul style="list-style-type: none"> <li>□ Mendocino Community Hospital</li> <li>□ Anderson Valley Health Center</li> <li>□ Redwood Coast Medical Services</li> <li>□ Mendocino Family Care</li> <li>□ Andy Coren, MD</li> <li>□ Mendocino County Department of Public Health</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>■ Browsersoft</li> <li>■ Business Networks International</li> <li>■ Center for Information Technology Leadership</li> <li>■ Children’s Hospital Informatics Program (CHIP) <ul style="list-style-type: none"> <li>□ IndivoHealth</li> <li>□ Automated Epidemiologic Geotemporal Integrated Surveillance System (AEGIS)</li> <li>□ Shared Pathology Informatics Network (SPIN)</li> </ul> </li>   <li>■ DB Consulting Group</li> <li>■ eHealth Initiative</li> <li>■ Electronic Health Record Vendors Association</li> <li>■ I2i Systems, Inc.</li> <li>■ GE Healthcare</li> <li>■ Initiate Systems</li> <li>■ Microsoft</li> <li>■ OpenHRE</li> <li>■ Regenstrief Institute</li> <li>■ SiloSmashers</li> <li>■ Sun Microsystems</li> </ul>

In Figure 4, the CSC-Connecting for Health team illustrates the prototype architecture deployed by the consortium. The capabilities are all contained in the facilities of subnetwork organizations (SNOs). These are somewhat analogous to the term NHIE used elsewhere in this report. The NHIN is simply the sum of all SNOs. In this prototype architecture, the NHIN is defined as a set of standards and practices by which all participating entities abide. There are no NHIN-level services or operators. Full details of this architecture can be found at [www.connectingforhealth.org](http://www.connectingforhealth.org).

**Figure 4. CSC Approach**



Source: CSC-Connecting for Health

Each SNO is configured differently in terms of where within the SNO the health information resides: Mendocino RHIO maintains data mirrors; IHIE maintains a data repository; MA-SHARE is configured to provide access to electronic health information at the CDO. Communications with an SNO flow organization to organization; communications between SNOs flow through Inter-SNO Bridges, which implement the security and auditing necessary for an SNO to communicate with its peer SNOs.

While the approach supports substantial heterogeneity in the architectures of the SNOs, each SNO must support a record locator service (RLS) for the records held by participating organizations. This service need only keep track of which systems may have data about a patient, and only records demographic information about the patient, without recording clinically disclosing information such as the types of tests or records held. Once the RLS provides record locations, those records are queried directly by the requester. This approach was adopted to leave the SNO less vulnerable to revealing protected health information through accidental disclosure or breaches of the RLS. The responsibility for filtering patient data is part of the data transfer between the holder and the requester of the data. Such filtering can be created by limiting which CDOs are queried, bracketing the time of the request or, where the quality of the metadata allows, limiting requests by clinical type.

The design of the system proceeded from a set of policy principles. A full accounting of these principles is available at <http://www.connectingforhealth.org>. For this report, Connecting for Health provided a summary of three of the principles that it considered most relevant to the prototype architecture. They are described here:

- Any network design must be widely adoptable. Large IT projects are hard, and the landscape is littered with epic failures. The U.S. healthcare system is idiosyncratic, with

*few sites that have infrastructure for hosting complex applications. As a result, the earliest instantiation of the NHIN must be the simplest possible version of that network, with all optional complexity postponed for later introduction. In particular, the architecture does not rely on the creation of new regional registries beyond the list of participating organizations, and the RLS.*

- *Patient privacy must be protected, even at the cost of some inefficiency. It is possible to imagine a network that stores and makes accessible all existing information about a patient from a central location, and such a system would have many desirable characteristics, but it would also create privacy risks. Care must be taken not to accidentally disclose sensitive information about the patient as a side-effect of the operation of the system. This includes the Record Locator Service, which should not include any clinical data, and the log files, which should likewise not be allowed to expose the contents of the records being logged.*
- *Finally, the combined requirements of simplicity and privacy suggest that the data about the patient (other than the minimum demographics required for identification) should remain in the care of institutions that generated the data or care for the patient (as with a lab and a doctor both retaining copies of test results.)*

### 2.2.3 IBM Prototype Architecture

As shown in Table 4, IBM worked with public health organizations as a partner as well as with a variety of provider organizations and RHIOs.

**Table 4. IBM Participants**

Healthcare Market	Technology Partners and Providers
<ul style="list-style-type: none"> <li>■ Research Triangle/Pinehurst, North Carolina— North Carolina Healthcare Information and Communications Alliance (NCHICA)                             <ul style="list-style-type: none"> <li>□ Duke University Health System                                     <ul style="list-style-type: none"> <li>– Durham Medical Center</li> </ul> </li> <li>□ FirstHealth of the Carolinas                                     <ul style="list-style-type: none"> <li>– Moore Free Care Clinic</li> <li>– Pinehurst Medical</li> <li>– Pinehurst Surgical</li> <li>– Southern Pine Women’s Center</li> </ul> </li> </ul> </li> <li>■ Rockingham County, North Carolina—NCHICA                             <ul style="list-style-type: none"> <li>□ Morehead Memorial Hospital                                     <ul style="list-style-type: none"> <li>– Eden Internal Medicine</li> <li>– Pulmonary, Allergy and Asthma Clinic of Danville</li> </ul> </li> <li>□ Moses Cone Health System                                     <ul style="list-style-type: none"> <li>– Family Tree OB/GYN</li> <li>– Moses Cone Internal Medicine Residency Program</li> </ul> </li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>■ Core Partners                             <ul style="list-style-type: none"> <li>□ CTIS</li> <li>□ Eclipse</li> <li>□ Initiate</li> </ul> </li> <li>■ Vendors                             <ul style="list-style-type: none"> <li>□ AllScripts</li> <li>□ Cisco</li> <li>□ CapMed</li> <li>□ GE Healthcare</li> <li>□ HealthVision</li> <li>□ LabCorp</li> <li>□ McKesson</li> <li>□ Meditech</li> <li>□ Possibility Forge (OpenEMR)</li> <li>□ Spectrum Labs</li> <li>□ SureScripts</li> </ul> </li> </ul>

Healthcare Market	Technology Partners and Providers
<ul style="list-style-type: none"> <li>■ Taconic Health Information Network and Community, Mid-Hudson Valley, (New York) <ul style="list-style-type: none"> <li>□ Kingston Hospital</li> <li>□ St. Francis Hospital</li> <li>□ Vassar Brothers Medical Center</li> <li>□ Physician Practices <ul style="list-style-type: none"> <li>– Hudson Valley Primary Care</li> <li>– Bridge Street Family Medicine</li> <li>– Springside Medical Associates</li> <li>– Rabi Sinha, MD</li> <li>– Hudson River Community Health</li> </ul> </li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>■ Other Organizations: <ul style="list-style-type: none"> <li>□ New York State Dept. of Health</li> <li>□ North Carolina Div of Public Health</li> </ul> </li> </ul>

In Figure 5, IBM provides an overview of its approach. The three levels are:

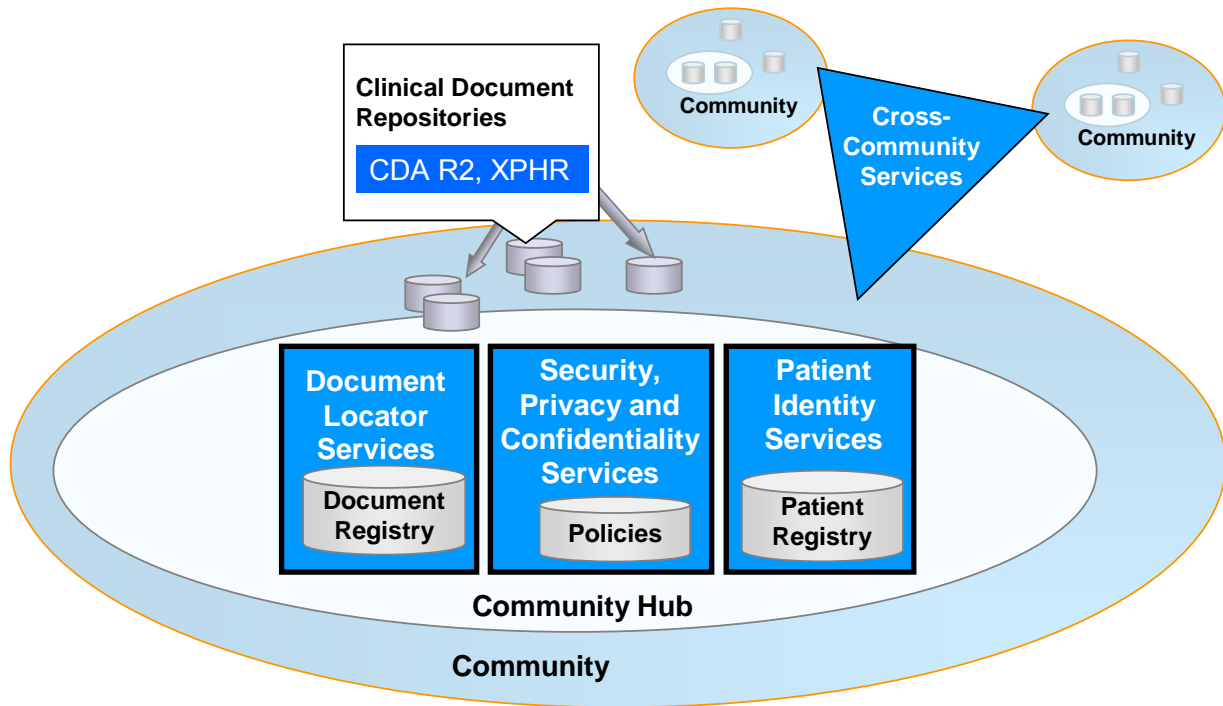
- The “community,” which represents all the organizations participating in an HIE
- The “community hub,” which provides the identity services and document locator services; and security, privacy and confidentiality service is necessary for an HIE to operate
- “Cross-community services,” which are the interconnections among the communities to achieve an NHIN

The cross-community services are implemented by agreed-upon standards among the communities. In this approach, community members may interact with one another directly, without having their interactions routed through special systems associated with the community hub. This reduces the potential for the community hub to become a bottleneck. At the same time, it requires more-widespread homogeneity with regard to exact conformance to standards.

This approach supports individual member organizations by providing clinical document repositories that may be deployed within the security boundaries of the member organizations. Where organizational characteristics dictate otherwise, the repositories could be maintained with the community hub.

The document locator service in this approach is supported by a registry that tracks individual reports or other clinical documents along with associated metadata. In so doing, it makes some of the distributed query use for information about a patient more efficient. At the same time, it may be regarded by some as increasing the danger of the privacy breach within the community hub.

**Figure 5. IBM Approach**



Source: IBM

**2.2.4 Northrop Grumman Prototype Architecture**

Table 5 lists the healthcare and technology partners in the Northrop Grumman consortium.

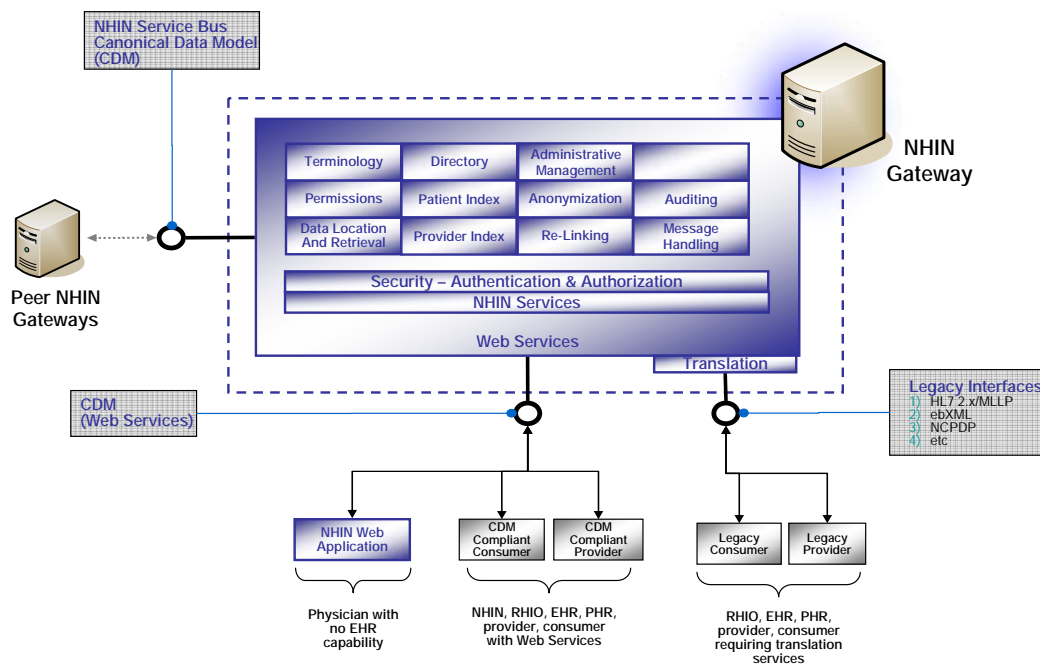
**Table 5. Northrop Grumman Participants**

Healthcare Market	Technology Partners and Providers
<ul style="list-style-type: none"> <li>■ Quality Health Network (Mesa County, Colorado)                             <ul style="list-style-type: none"> <li>□ St. Mary’s Hospital</li> <li>□ Rocky Mountain Health Plan Community Hospital</li> <li>□ Primary Care Partners</li> </ul> </li>   <li>■ Santa Cruz RHIO (Santa Cruz, California)                             <ul style="list-style-type: none"> <li>□ Dominican Hospital</li> <li>□ Reference Labs (Quest, Stanford, Hunter, APMG)</li> <li>□ RMG</li> <li>□ Physicians Medical Group</li> <li>□ Western Medical Associates</li> </ul> </li>   <li>■ University Hospitals Health System (Cleveland, Ohio)                             <ul style="list-style-type: none"> <li>□ Community Hospitals</li> <li>□ Outpatient Centers</li> <li>□ MacDonald Women’s Hospital</li> <li>□ Rainbow Babies and Children’s Hospital</li> <li>□ Ireland Cancer Center</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>■ Axolotl</li> <li>■ Client/Server Software Solutions</li> <li>■ First Consulting Group</li> <li>■ Oracle</li> <li>■ RxHub</li> <li>■ SeeBeyond Technology, Sun Microsystems</li> <li>■ SphereCom Enterprises</li> </ul>

In Figure 6, Northrop Grumman describes its approach. It is a service-oriented architecture, based on the following principles:

- Achieve broad nationwide interoperability by leveraging existing interoperability—reduce the need to “rip and replace” existing HIEs, instead providing mediation services
- Eliminate dependence on centralized nationwide services
- Enable interoperability across different information domains (such as laboratory, medications, public health, etc.) through the use of a canonical information model, such as the HL7 Reference Information Model

**Figure 6. Northrop Grumman Approach**



Source: Northrop Grumman

Northrop Grumman describes the architecture as based on a “super-peer” topology. Not all service providers and consumers will be connecting directly to each other as peers, but a smaller subset of the services will connect together at the top of the hierarchy as super-peers. These super-peers all expose a minimal set of core services, which is logically aggregated in what they called an NHIN Gateway, a system that provides many of the features of NHIEs described in this document.

Figure 6 summarizes the components of the NHIN Gateway. These are logical components, which could be realized within a single collected hardware platform or across multiple platforms. The NHIN Gateways expose two main sets of interfaces: (1) NHIN Gateway peer-facing interfaces, which represent the key high-level interactions that define an NHIN, and which need to be strictly controlled through standards and certifications, and (2) NHIN Gateway children-facing interfaces, which apply within that particular HIE, and which may be able to adapt to systems that have interfaces that do not yet meet the NHIN standards. This assistance is particularly likely to be required in the evolution of the NHIN.

The core services included in the NHIN Gateway concept are:

- Patient Identification
- Provider Identification
- Data Location and Retrieval
- Anonymization and Relinking
- Directory
- Terminology Mediation
- Message Handling (includes transformation, routing, guaranteed delivery and content-based filtering)
- Auditing
- Authentication and Authorization
- Permissions Management
- Administrative Management (includes activity monitoring, configuration, service-level agreement enforcement and performance monitoring)

The Permissions Management service provides a mechanism for patient permission preferences to be stored and maintained, and thus applied separately from a particular PHR or other mechanism used to enter such preferences. The Directory service refers to a registry of entities (care organizations, ancillary result centers, hospitals, etc.) that are directly connected to each gateway, allowing those organizations and their systems to be found during queries. The architecture suggested a replication scheme in which new organizations or entities would register themselves with the local gateway, after which this information would be replicated and made available to other gateways nationwide (analogous to the manner in which the Internet's Domain Name Servers work).

## 2.3 Summary of Accomplishments

Contractors provided deliverables in four forms: (a) written reports; (b) presentations; (c) discussions at three NHIN forums; and (d) a demonstration of interactions among their communities at the Third NHIN Forum. In addition, they often collaborated informally at national meetings on HIEs and the NHIN.

The content of these deliverables provides insight into the rationales, approaches and recommendations of the four efforts that will be useful for the trial implementations and other early adopters of the NHIN.

They each contributed source data to the analysis of NHIN functional requirements that was conducted by the National Council on Vital Statistics<sup>8</sup>.

Each of the prototype architectures:

- Showed the synergies of supporting consumers and providers on the same infrastructure

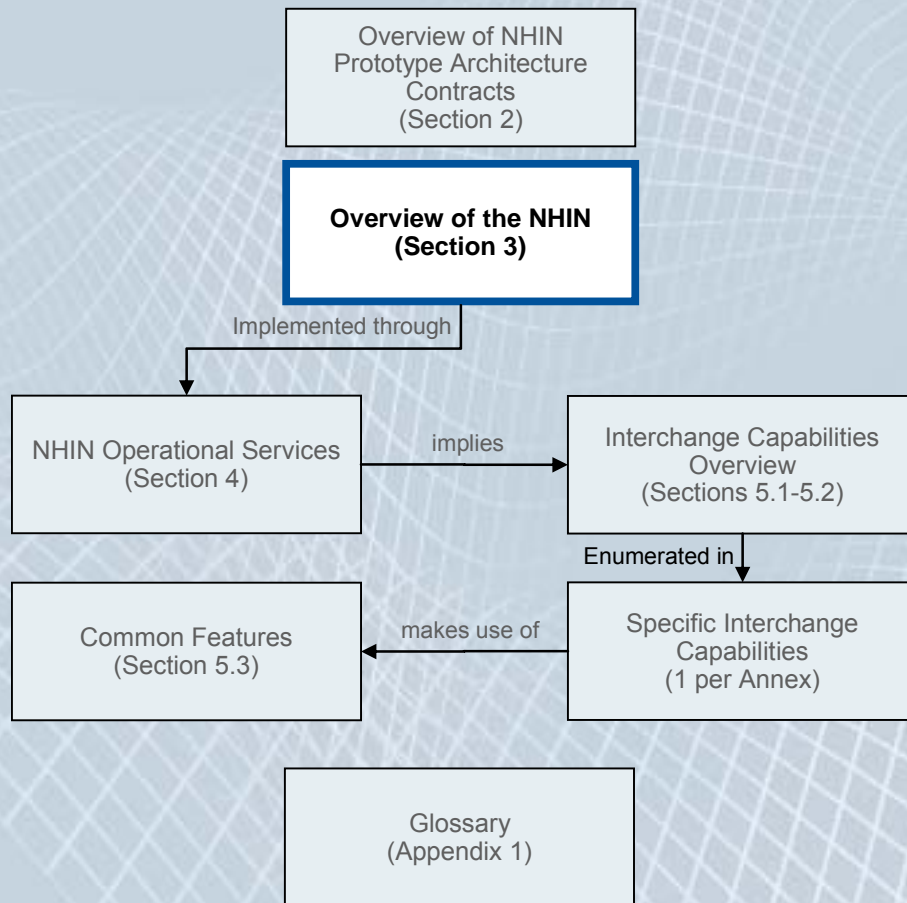
---

<sup>8</sup> "Report to the Secretary of the U.S. Department of Health and Human Services on Functional Requirements Needed for the Initial Definition of a Nationwide Health Information Network (NHIN)," National Committee on Vital and Health Statistics, October 30, 2006.

- Demonstrated PHRs and EHRs interoperating
- Showed approaches for nationwide health information sharing that did not depend on a national patient identifier
- Met the contract requirements with expected variations in where and how the services could be implemented
- Showed architectures that supported heterogeneous technological solutions at the level of the NHIE and the systems of the participating care delivery or consumer organizations
- Validated the notion that the NHIN does not require centralized operations
- Showed approaches to building an NHIN that were supportive of a migration to standard interfaces, rather than requiring wholesale updating of the participants' systems to get started

Their approaches have coalesced into the going-forward approach being adopted by the ONC in support of the next steps in building an NHIN that is responsive to the priorities set forth by the AHIC.

## ■ ■ ■ ■ An Overview of the NHIN



## 3.0 An Overview of the NHIN

This section provides an overview of the NHIN that arises from the NHIN Prototype Architecture Contracts and other inputs. It expands on the information provided in the Executive Summary.

### 3.1 Benefits

In describing the importance of Healthcare IT, Secretary Michael Leavitt identified these benefits, most of which rely in some way on the NHIN:

- To the healthcare consumer:
  - Higher-quality care
  - Reduction in medical errors
  - Fewer duplicate treatments and tests
  - Decrease in paperwork
  - Lower health-care costs
  - Constant access to health information
  - Expansion of access to affordable care
- To public health:
  - Early detection of infectious disease outbreaks around the country
  - Improved tracking of chronic disease management
  - Ability to gather de-identified data for research purposes
  - Evaluation of healthcare based on value, enabled by the collection of price and quality information that can be compared<sup>9</sup>

### 3.2 Constituents of the NHIN

The NHIN will be a “network of networks” that securely connects consumers, providers and others who have, or use, health-related data and services, while protecting the confidentiality of health information. The NHIN will not include a national data store or centralized systems at the national level. Instead, the NHIN will use shared architecture (standards, services and requirements), processes and procedures to interconnect health information exchanges and the users they support.

Many of the stakeholders in healthcare already have networks for operating within large organizations or proving connections among them for specific purposes. The NHIN is not intended to supplant these networks. They will continue to handle the bulk of day-to-day transactions in providing and measuring healthcare. Instead, the NHIN is a “network of networks,” built over the Internet.

#### 3.2.1 The Health Information Exchange

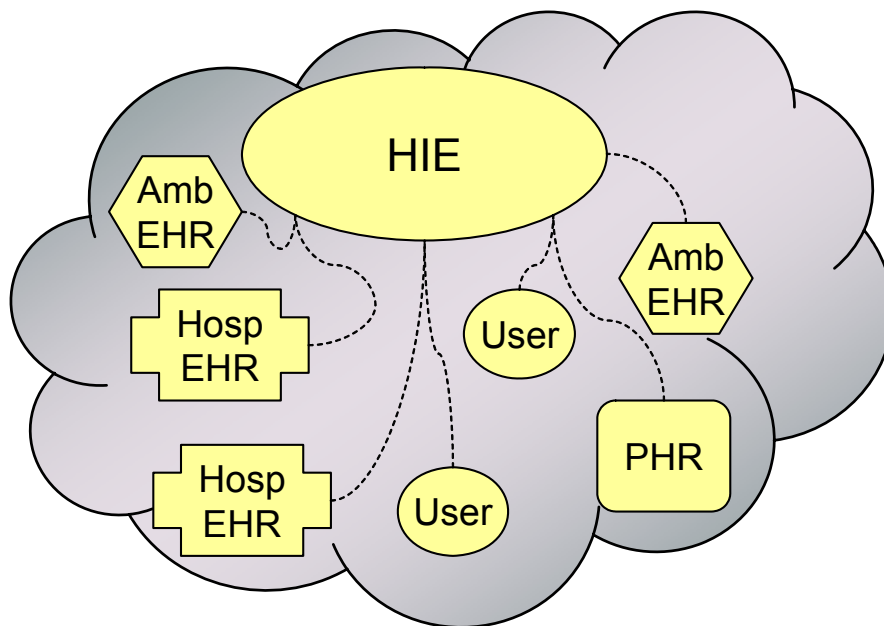
HIEs are organizations that enable the movement of health-related data among other organizations within a state, a region or a non-jurisdictional participant group. HIEs generally

---

<sup>9</sup>Leavitt, *ibid.*

include, or are supported by, governance, operations and technical capabilities. The users of an HIE will include organizations that have their own EHRs, PHRs or other clinical systems, and individuals who cannot access the HIE through the systems of the organizations with which they work. These latter individuals may gain access to shared information, subject to appropriate privacy and security protections, through portals operated by the HIE. What is likely to be a typical HIE is graphically represented in Figure 7.

**Figure 7. A Health Information Exchange**



An important core competency of the HIE is to maintain a trusting and supportive relationship with the organizations that provide data to, and retrieve data from, one another through the HIE. The trust requirement is met through a combination of legal agreements, advocacy and technology for ensuring meaningful information interchange in a way that has appropriate protections.

The organizations that operate the EHRs will have a variety of heterogeneous systems built on varying technologies. Many of these EHRs will not be standard in the manner by which they internally represent clinical information. Most current HIEs do, and many new ones may, support the member organizations that have these EHRs by providing assistance in mapping the interchanged data from an organization-specific format into standard format.

### 3.2.2 The NHIN Health Information Exchange

An HIE by itself can only support information interchange among the members of the HIE. The NHIN will be the link that enables extending information exchange to members of other HIEs. In order to participate in the NHIN, the HIE will need to meet specific requirements, such as:

- Supporting secure operation in all activities related to the NHIN
- Protecting the confidentiality of personally identifiable health information as it is used by those who participate in the NHIN
- Reconciling patient and provider identities without creating national indices of patients
- Providing local registries that may be used, when authorizations permit, to find health information about patients

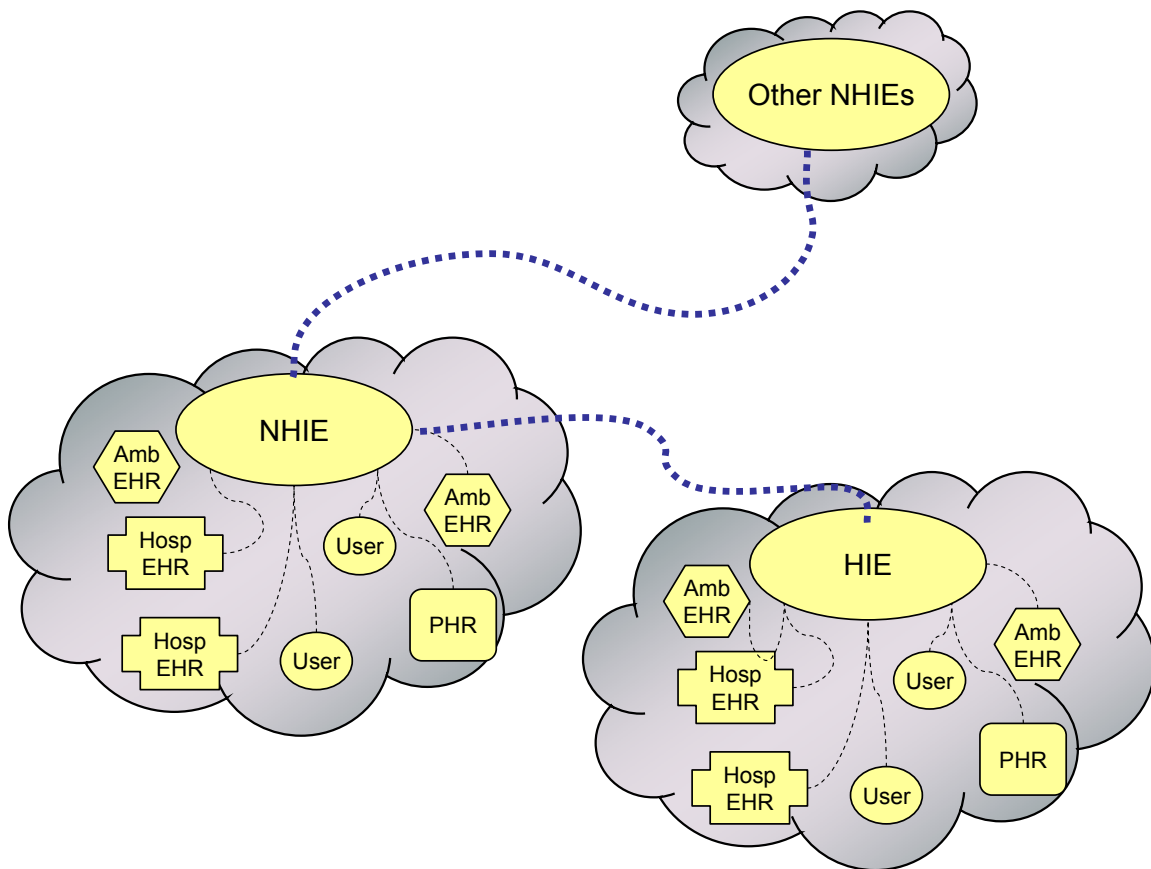
- Supporting the transfer of information from one provider or care delivery organization in support of collaborative care
- Supporting secondary uses of data while protecting the identity of patients to the degree required by law and public policy

While these requirements are not conceptually different from those needed by any HIE, participating in the NHIN implies that the requirements must be met in a uniform way. An HIE that meets the NHIN architecture (services, standards and requirements), policies and procedures is referred to as an NHIE.

A critical component of the NHIN architecture is the NHIN Operational Services. They are discussed in more detail in Section 4.1 of this report.

Not every HIE may choose to invest in all the technology and staff required to meet the requirements of an NHIE. There is a path for the users of such an HIE to experience data exchange using the NHIN. Such an HIE may rely on another HIE, as shown in Figure 8.

**Figure 8. An NHIE Supporting Another HIE**



Under this architecture it is possible that an NHIE might be created solely for the purpose of supporting other HIEs. Under such an approach the NHIE might directly provide some of the operational services while providing other operational services indirectly through the activities of the participating HIEs. For example, a statewide NHIE might provide secure connections to other NHIEs and the patient registry while the connections to EHRs, PHRs and other registries

might be provided for various regions within a state. While this approach is supported, it is not required.

### **3.2.3 Specialized NHIN Participants**

Not all organizations that exchange information through the services of the NHIN will be care delivery organizations with EHRs, consumer organizations with PHRs or HIEs. Other organizations may participate, including those that focus on:

- Public health
- Quality assessment
- Clinical research
- Specialty networks such as healthcare clearinghouses

Depending on their geographical scope, these organizations may participate in the NHIN by using the services of an NHIE. Sometimes, however, it may make more sense for them to directly participate as a peer with NHIEs. The specialized nature of these organizations means that they may require a subset of the shared architecture (standards, services and requirements), processes and procedures used by the other participants. The subset requirements have not yet been determined.

### **3.2.4 Health Information Service Providers (HSPs)**

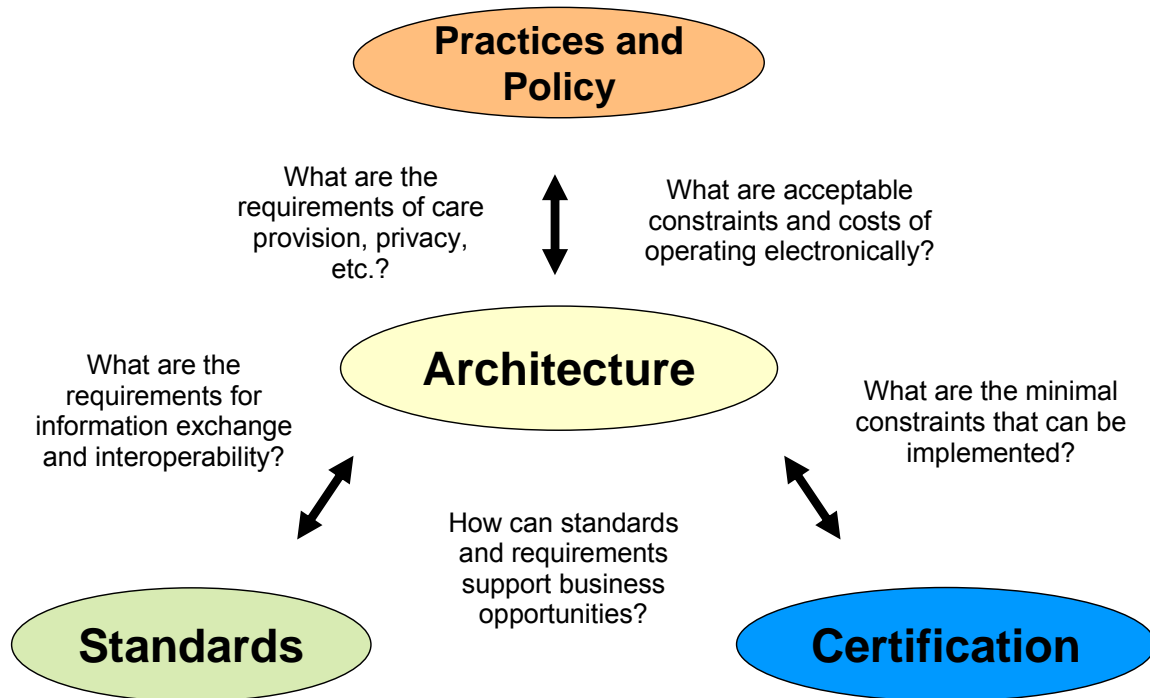
An HIE that chooses to become an NHIE will not need to develop or operate all the software itself or even to use its own staff to provide the required operational services. As with any other IT user, it may choose to work with a third party for software, computer operations and other operational services. The third party may be a commercial firm, an agency of some level of government or a non-profit organization. Such third-party service providers are called HSPs in the context of the NHIN.

A specialized NHIN participant may also operate as a peer with other NHIEs by using the services of an HSP.

Note that an HSP itself will not be a direct organizational participant in the NHIN. It will provide services to the NHIE or specialized entity that is the actual NHIN participant.

## **3.3 Related ONC Initiatives**

As described in the Executive Summary, Section 1.1, architecture is related to and informs three other concepts important to the NHIN: policy, standards and certification. Figure 9 illustrates this relationship. Policy informs architecture by identifying specific requirements that must be met by systems implemented according to the architecture. Of course, some policies are more costly to implement than others. For example, some policies may require more attention by people to the process of exchanging health information. While it is the primary goal of architecture to implement standards, on occasion the architecture process should provide feedback to policymakers on the consequences of policies being considered.

**Figure 9. The Relationship of Architecture to Other NHIN Initiatives**

Source: ONC

### *Practices and Policy*

The NHIN architecture must be strongly related to policy. Policy informs architecture by identifying specific requirements that must be met by systems implemented according to the architecture. Architecture informs policy and policy development by enabling policymakers with approaches and solutions. In the U.S. today, however, there is substantial heterogeneity among the laws and regulations of the states, and many policies were developed during a time when information sharing was primarily done on paper or by fax. The ONC has several initiatives under way to create more consensus on policy issues and to update policies based on the threats and limitations of electronic information exchange. The Health Information Security and Privacy Collaboration (HISPC) and the National Governors Association State Alliance for e-Health are ONC initiatives that are focused on bringing consensus to policy issues.

Because this is a sensitive area, and because the potential impact of policy options is not always understood, the relationship between architecture and policymaking is bidirectional. The architecture must have the flexibility to accommodate changes in policy that will be identified in the future. At the same time, the industry must acquire enough experience with the architecture to realistically predict the costs of various approaches. Approaching policy and architecture issues in parallel is the only viable approach to sorting out complex, sensitive issues for large-scale systems.

If it were practical to develop a challenging initiative such as the NHIN “top-down,” its architecture would be developed based on a thorough understanding of a consistent set of policies and best practices around privacy, security, patient identification and many other operational aspects of an NHIN; standards would be developed to correspond to the

architecture; and the means of certifying that organizations meet NHIN requirements would be developed after the standards and architecture were in place.

However, that approach is not realistic. The NHIN approach is a best practice: to address these endeavors in parallel with policy coordination.

### *Standards*

In a “top-down” world, standards would be developed to support the interfaces identified by architectural analysis. The real world, however, is far more complex. Standards development is a very exacting process with a multiyear lead time between project initiation and full realization in systems in widespread operation. To be effective, architecture both informs the selection of standards to be developed, and recognizes the opportunities of standards that are in place. This is particularly important when supporting the “no rip-and-replace” requirement.

A second issue with standards is that there are many standards that cover different aspects of health information exchange. It takes a concerted effort to bring several standards together in order to achieve full interoperability. For example, laboratory data specifications will combine a format from one standards organization with codes from two or more other standards organizations, and may rely on yet another organization to provide the standards necessary to achieve confidentiality, reliability and security. Finally, on occasion multiple standards development organizations will have produced standards for the same purpose.

To achieve interoperability, there must be a consensus process for choosing among standards and then describing exactly how to detail, constrain and combine them to achieve a specific purpose. The [Healthcare Information Technology Standards Panel](#) (HITSP) was founded by the ONC with the purpose of developing these consensus positions.

### *Certification*

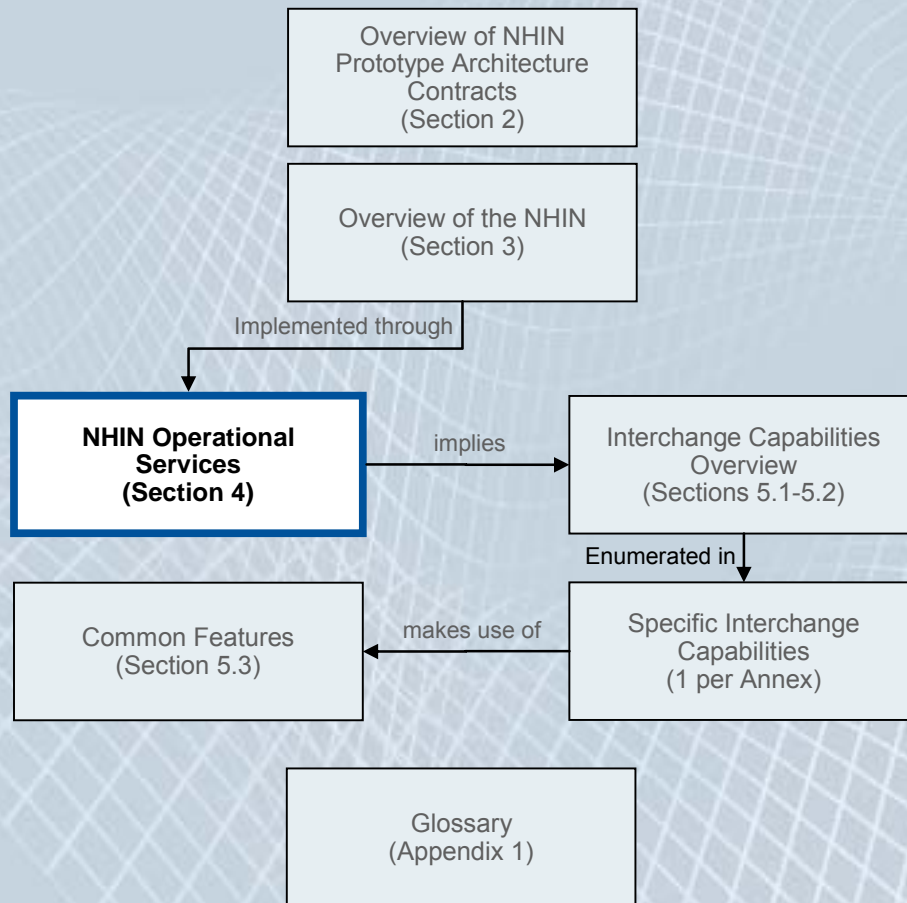
IT standards are notoriously hard to implement when the products of separate organizations must interoperate. Many users of personal computers can remember the early days of the Universal Service Bus (USB) standard when each “plug and play” device required hours searching the Web or talking to a vendor’s technical support staff to go from “plug” to “play.” Currently, most USB devices can be installed in a very smooth process. The difference is a concerted industry effort to certify conformance to the USB standards by actually testing devices before they are released to the market. Finally achieving this interoperability has enabled an increase in the products available to the marketplace.

The [Certification Commission for Healthcare Information Technology](#) (CCHIT) is an organization established by The American Health Information Management Association, The Healthcare Information and Management Systems Society and The National Alliance for Health Information Technology, with the support of ONC to provide the certification function for the functionality, interoperability and security of certain classes of healthcare systems. In 2008, CCHIT contemplates including the certification of systems as participants the NHIN.

### *Overall Coordination*

The [American Health Information Community](#) (AHIC) is a blue-ribbon panel of senior executives representing consumers, employers, healthcare providers, healthcare payers and public health in private industry and government. Its role is to advise the Secretary in establishing initiatives and setting priorities for efforts to improve the use of healthcare IT. One of its primary means of communicating priorities is through breakthrough/use cases—formalized descriptions of specific usages of healthcare IT scenarios that represent important advances in the use of IT to improve healthcare.

## ■ ■ ■ ■ NHIN Operational Services



## 4.0 NHIN Operational Services

In order to be participant in the NHIN, an NHIE will need to provide certain operational services<sup>10</sup>. One example would be proofing the identity of a proposed user. Another would be dealing with security incidents.

Many operational services are provided by networking among the NHIEs. An example of this would be the service of locating clinical information about a patient. An NHIE may offer these services in two ways:

- A person who is a user of the NHIE may access such a service while using a portal provided by the NHIE
- A person who is a user of a PHR, EHR or other system that is connected to the NHIE may perform a function in the application system that causes the application system to request the information on a computer-to-computer basis using the service of the NHIE

The set of operational services that an HIE will need to provide in order to be an NHIE are referred to as the “NHIN Operational Services.”

When an operational service includes the requirement for communication among NHIEs, the NHIEs will be required to intercommunicate in a standard way. That is to say, they all will need to use a common set of interfaces. When an operational service will be fulfilled in part using such an interface, we say that the operational service implies an interface. This terminology is chosen to describe the multi-way association between operational services and interfaces. Not every operational service will require an interface. Those that do may require the use of one or more interfaces to fulfill their requirements.

In Section 4.1 we enumerate the list of core services that were developed through the experience of the NHIN prototype architecture contracts and through other activities that occurred in the same time frame. In Section 4.2 we list the interfaces that are implied by specific operational services. Those interfaces are actually described in annexes that appear at the end of this document.

### 4.1 Operational Services

The NHIN operational services are listed in Table 6.

---

<sup>10</sup> The term “services” is used in very different ways by general readers and network architects. In describing NHIE operational services, we are using the general sense of the word: “...an act or a variety of work done for others.”

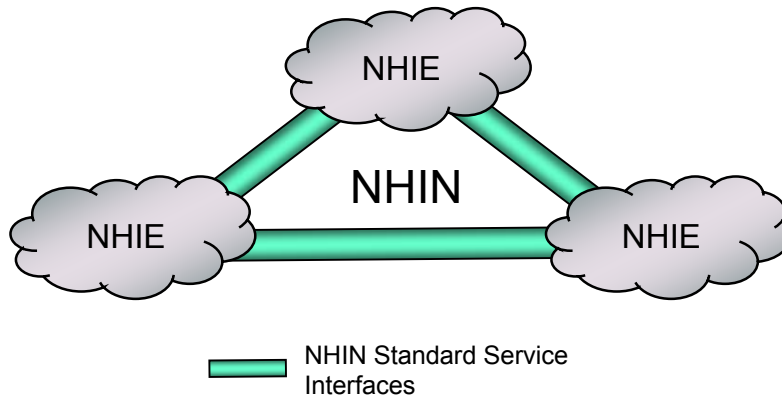
**Table 6. NHIN Core Services and Capabilities**

<b>Core Services and Capabilities</b>	
<b>Data Services</b>	<ul style="list-style-type: none"> <li>■ Secure data delivery, and confirmation of delivery, to EHRs, PHRs, other systems and networks</li> <li>■ Data look-up, retrieval and data location registries</li> <li>■ Support for notification of the availability of new or updated data</li> <li>■ Subject-data matching capabilities</li> <li>■ Summary patient record exchange</li> <li>■ Data integrity and non-repudiation checking</li> <li>■ Audit logging and error handling for data access and exchange</li> <li>■ Support for secondary use of clinical data including data provisioning and distribution of data transmission parameters</li> <li>■ Data anonymization and re-identification as well as HIPAA de-identification</li> </ul>
<b>Consumer Services</b>	<ul style="list-style-type: none"> <li>■ Management of consumer-identified locations for the storage of their personal health records</li> <li>■ Support of consumer information location requests and data routing to consumer-identified personal health records</li> <li>■ Management of consumer-controlled providers of care and access permissions information</li> <li>■ Management of consumer choices to not participate in network services</li> <li>■ Consumer access to audit logging and disclosure information for PHR and HIE data</li> <li>■ Routing of consumer requests for data corrections</li> </ul>
<b>User and Subject Identity Management Services</b>	<ul style="list-style-type: none"> <li>■ User identity proofing and/or attestation of third-party identity proofing for those connected through that HIE</li> <li>■ User authentication and/or attestation of third-party authentication for those connected through that HIE</li> <li>■ Subject and user identity arbitration with like identities from other HIEs</li> <li>■ Management of user credentialing information (including medical credentials as needed to inform network roles)</li> <li>■ Support of an HIE-level, non-redundant methodology for managed identities</li> </ul>
<b>Management Services</b>	<ul style="list-style-type: none"> <li>■ Management of available capabilities and services information for connected users and other HIEs</li> <li>■ HIE system security including perimeter protection, system management and timely cross-HIE issue resolution</li> <li>■ Temporary and permanent de-authorization of direct and third-party users when necessary</li> <li>■ Emergency access capabilities to support appropriate individual and population emergency access needs</li> </ul>

## 4.2 The Role of Interoperability in Supporting Operational Services

Many of the operational services can only be implemented through interfaces between the systems of the cooperating NHIEs. Because there are potentially many NHIEs, it would not be feasible for them to negotiate their interfaces bilaterally. Instead, each NHIE will need to follow the standard interfaces exactly. Figure 10 illustrates this relationship.

**Figure 10. NHIN Standard Interfaces**

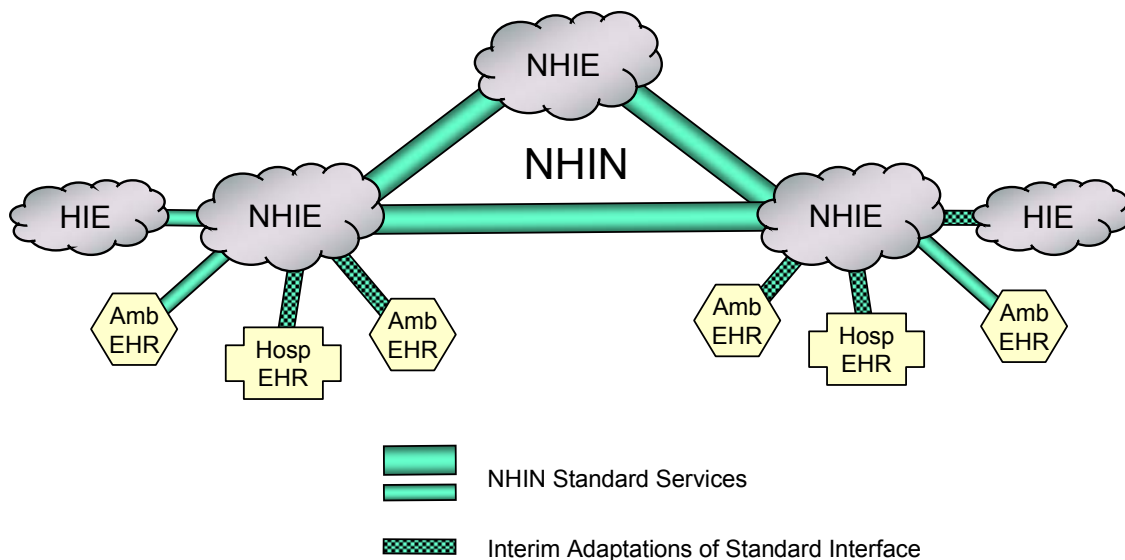


Many of the standard interfaces that will be used among NHIEs will also be suitable for use between an NHIE and an HIE, or between an NHIE and the PHR or EHR of a participant in the NHIE. However, it is expected that there may be a period of time before the systems of an HIE participant organization are fully capable of using the standard interfaces. An NHIE may choose to offer additional services that support the participation of less-standard systems in the NHIN. Some examples of the optional services that an NHIE might offer include:

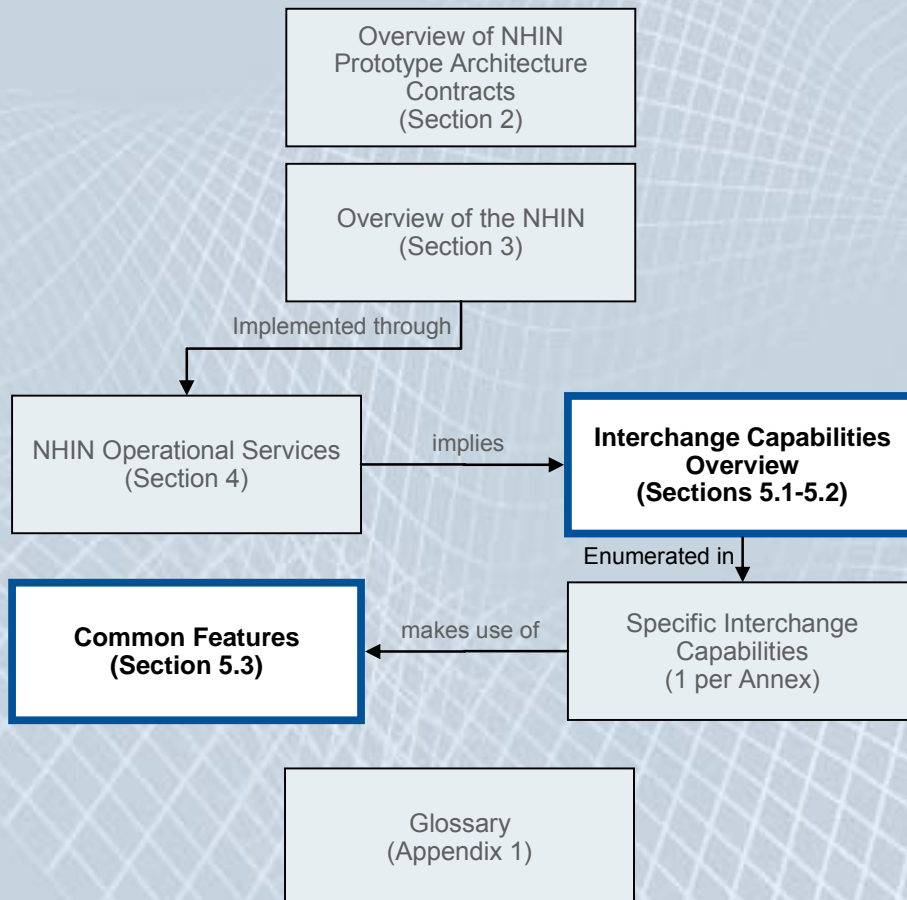
- Terminology mapping
- Message construction and transformation
- Data filtering
- Data de-identification
- Data pseudonymization
- Support of authorized re-linking of data

Figure 11 illustrates the extended use of standard interfaces and other interfaces supported by optional NHIE services for adapting existing systems.

**Figure 11. NHIE Value-Added Services: Adapted Interfaces**



## ■ ■ ■ ■ Interchange Capabilities



## 5.0 Interchange Capabilities

Interchange capabilities are collections of interfaces that cluster around specific operational services. Section 5.1 identifies the operational services that will be required of NHIEs. The operational services are treated in this document as described in Table 7.

**Table 7. Treatment of Operational Services in This Document.**

Aspect of an Operational Service	Treatment in This Document
Operational services imply standard interfaces among computers that communicate through NHIEs.	Interfaces are described in the annexes to this document.
Operational services imply features that are common to many interfaces but do not imply specific standard interfaces.	Common features are named and described in Section 5.2.2; the names of relevant common features are listed in each annex.
Operational services imply requirements of an NHIE that are unrelated to computer-to-computer interfaces.	Not further described in this document.

Each annex describes an interchange capability. This section provides general material that applies to all the annexes.

### 5.1 Operational Services vs. Interchange Capabilities

Table 8 presents the primary relationship between NHIN operational services and the annexes that define interchange capabilities. Where the operational service does not imply a particular interchange capability but is primarily related to some of the common features, those features appear in this table in lieu of a reference to an annex. However, even where an operational service is implied by an interchange capability, common features are implied. The linkage between a specific interchange capability and a common feature appears in a table at the end of each annex.

**Table 8. Operational Services, Interchange Capabilities and Common Features**

Operational Service	Implies Interchange Capability or Common Features
<b>Consumer Capabilities</b>	
Management of consumer-identified locations for the storage of their personal health records	Annex 9. Pseudonymize and Re-Identify Data
Support of consumer information location requests and data routing to consumer-identified personal health records	Annex 2. Identify Subject Annex 14. Route Data Based on Consumer-Specified Preferences
Management of consumer-controlled providers of care and access permissions information	Annex 4. Maintain Consumer Data Sharing Permissions
Management of consumer choices to not participate in network services	Annex 4. Maintain Consumer Data Sharing Permissions
Consumer access to audit logging and disclosure information for PHR and HIE data	Annex 7. Provide Consumer Access to Access and Disclosure Logs
Routing of consumer requests for data corrections	Annex 12. Route Consumer Request to Correct Data

Operational Service	Implies Interchange Capability or Common Features
<b>Data Services</b>	
Secure data delivery, and confirmation of delivery, to EHRs, PHRs, other systems and networks	5.3.4 Data Integrity Checking 5.3.5 Error Handling 5.3.8 Non-repudiation 5.3.9 Patient Summary Record Support
Data look-up, retrieval and data location registries	Annex 3. Locate Records
Support for notification of the availability of new or updated data	Annex 13. Route Data Annex 14. Route Data Based on Consumer-Specified Preferences
Subject-data matching capabilities	Annex 1. Arbitrate Identity Annex 2. Identify Subject
Summary patient record exchange	Annex 11. Retrieve Data
Data integrity and non-repudiation checking	5.3.4 Data Integrity Checking and 5.3.8 Non-repudiation
Audit logging and error handling for data access and exchange	5.3.1 Audit Logging 5.3.5 Error Handling
Support for secondary use of clinical data including data provisioning and distribution of data transmission parameters	Annex 6. Manage Data Selection Parameters for Secondary Use Annex 8. Provide Data to Secondary Users Annex 9. Pseudonymize and Re-Identify Data
Data anonymization and re-identification as well as HIPAA de-identification	Annex 9. Pseudonymize and Re-Identify Data 5.3.6 HIPAA De-Identification
<b>User and Subject Identity Management Services</b>	
User identity proofing and/or attestation of third-party identity proofing for those connected through that HIE	5.3.12 Transmit Disambiguated Identities
User authentication and/or attestation of third-party authentication for those connected through that HIE	5.3.2 Authentication (Person) 5.3.12 Transmit Disambiguated Identities
Subject and user identity arbitration with like identities from other HIEs	Annex 1. Arbitrate Identity Annex 2. Identify Subject
Management of user credentialing information (including medical credentials as needed to inform network roles)	5.3.12 Transmit Disambiguated Identities
Support of an HIE-level, non-redundant methodology for managed identities	5.3.12 Transmit Disambiguated Identities
<b>Management Services</b>	
Management of available capabilities and services information for connected user organizations and other HIEs	Annex 5. Maintain Registries of NHIN-Participating Systems and Organizations

Operational Service	Implies Interchange Capability or Common Features
HIE system security including perimeter protection, system management and timely cross-HIE issue resolution	(Not primarily related to interchange capabilities)
Temporary and permanent de-authorization of direct and third-party users when necessary	Annex 2. Identify Subject
Emergency access capabilities to support appropriate individual and population emergency access needs	Annex 4. Maintain Consumer Data Sharing Permissions

## 5.2 Annex Format

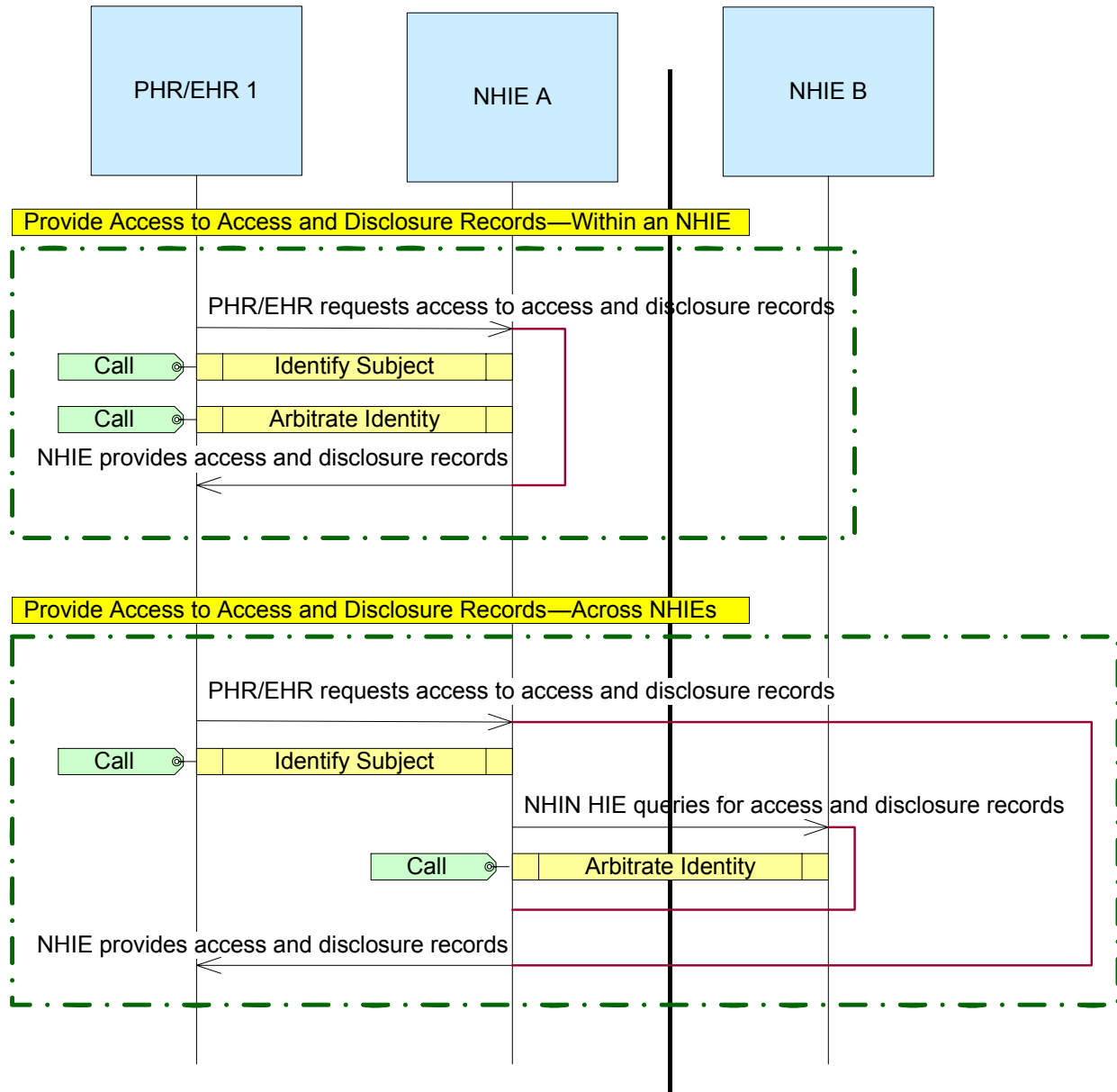
Each annex describes a specific interchange capability. It includes:

- A unique descriptive name, which is the title of the annex
- A description
- An illustrative example
- A diagram of the sequences of actions that are the interchanges described by the annex (this is sometimes called the “choreography”)
- A more specific description of the actions that constitute the protocol
- A listing of common features that apply to the transactions
- A listing of registries that are relevant to the interchange capability

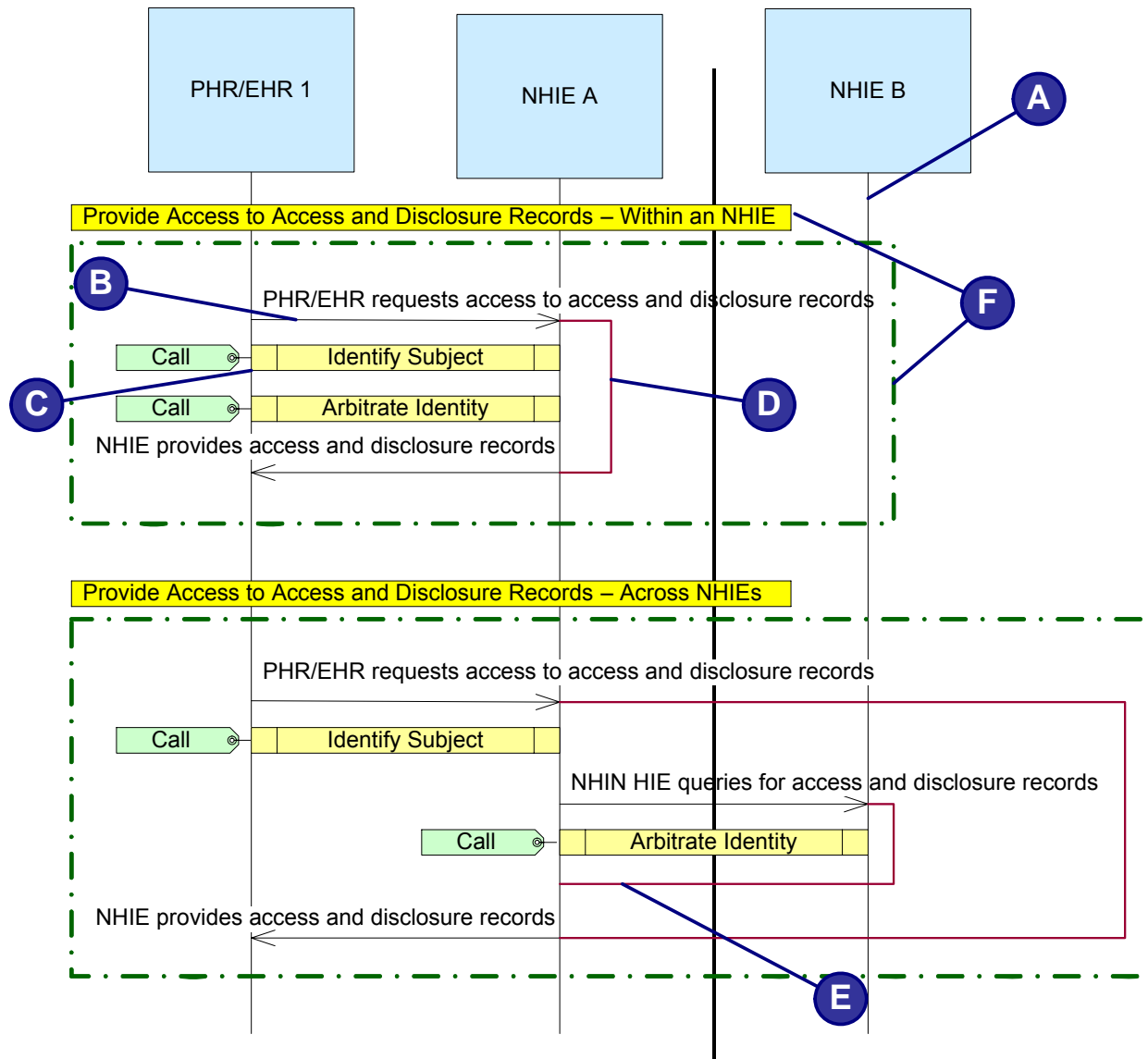
Note that the word “subject” has a very specific meaning in these annexes. It represents an entity identified within a message or a query. Subjects include patients and providers. Although the terms “patient” and “consumer” usually refer to the same class of person, this report uses “consumer” to refer the person who directly or indirectly uses the NHIN and “patient” to the entity described in messages with clinical data.

Figure 12 is an example of an annex diagram. Figure 13 adds annotations to Figure 12.

Figure 12. An Example of an Annex Diagram



**Figure 13. Annotated Example of Annex Diagram**



<p><b>A</b></p>	<p>Each solid vertical line is headed by a box that represents the types of systems that will participate in the NHIE:</p> <ul style="list-style-type: none"> <li>■ An EHR</li> <li>■ A PHR</li> <li>■ Another kind of clinical information system such as a laboratory information system</li> <li>■ Any of several systems that may be operated on behalf of the NHIE itself</li> </ul>
<p><b>B</b></p>	<p>An arrow represents an action that will be conveyed from one of the systems to another. The actions are named and further described in the subsection of the annex that follows the diagram. Actions are only included if they would likely convey some application data between systems. In omitting simple acknowledgements, this high-level view leaves the question of whether the communications are synchronous to design processes that will occur in the ongoing development of the NHIN.</p>

<b>C</b>	A box with a tag labeled Call represents a group of actions that are defined in another annex. The name of the annex is within the box. The actions from the other annex should appear in the sequence of actions where the box is positioned.
<b>D</b>	A bracket groups two or more actions into a transaction, a logical grouping of actions that must all succeed or fail as a group <sup>11</sup> .
<b>E</b>	When the action that completes a transaction is a simple acknowledgement, there is no arrow for it, as described above, at B. In this case, the leg of the bracket that would connect with an arrow is extended as shown here.
<b>F</b>	A box drawn with green broken lines encloses a transaction package, a group of transactions that are used to support a stand-alone information exchange between two or more systems <sup>2</sup> . A label above the transaction box provides a name for the transaction package. When a tag with the word “foundational” is attached to a transaction package, that package serves to provide a context for other transaction packages in the diagram. This is further explained in Section 5.2.1.

### 5.2.1 Foundational Transaction Packages

A foundational transaction package represents transactions that are logical precursors to the transaction packages that are the main subject of the annex. For example, in Annex 2. Identify Subject, the main subject of the annex is a transaction package that is also named Identify Subject. This is the transaction package that is used in some circumstances to look up a patient or other subject from a registry that has been established by the NHIE. The Annex also includes foundational transaction packages for an initial load of the subject registry and subsequent updates.

### 5.2.2 NHIE Logical Registries

In order to describe the logic of transactions in the annexes, there is an assumption that certain classes of data will be retained on behalf of the NHIE. These logical classes of data are described as registries. Their being mentioned in the annexes should not be taken to imply where or how this information is stored. As used in this report, the term is unrelated to clinical information systems such as tumor registries.

The logical registries that were identified are described in Table 9.

**Table 9. NHIE Logical Registries**

<b>Consumer</b>	Consumers as they may be identified in PHRs or directly in the enabling systems of the NHIE
<b>Patient</b>	Patient identities as required to correlate slight variants of the identifying information that may occur when the consumer is the subject of clinical information
<b>Provider</b>	Healthcare providers that may be designated to receive or access patient information
<b>PHR Record Location</b>	Designated target for information about a consumer for the transfer of data to the consumer’s PHR and for queries of data in a PHR
<b>EHR Record Location</b>	The locations of EHRs or organizations that may be able to provide or receive clinical information about a patient

<sup>11</sup> Adapted from HITSP, “HITSP Interoperability Specification: Harmonization Framework, v1.1”, 12 Sept 2006, p 1.

<sup>2</sup> Adapted from HITSP, *ibid.*

<b>Consumer Permissions</b>	Consumers' specification of providers who may view or access their PHR data
<b>Organizational Participant</b>	Organizations that participate within an NHIE
<b>System/Network</b>	Systems and networks that may send data to, or receive data from, an NHIE

## 5.3 Common Transaction Features

Here we describe features that are common to multiple annexes. In this section, the phrase “participating system” refers to any system that sends or receives information to or through the NHIE. These systems may be operated by members of HIEs or the NHIE itself.

Many of the operational services that imply a computer-to-computer service may also be offered to people through portals operated by the NHIE. The systems that implement those portals must meet the same requirements as any participating EHR, PHR or other clinical information system.

### 5.3.1 Audit Logging

NHIEs shall create audit logs of actions taken by the NHIE in response to queries and in managing data sent to or through them for the purpose of maintaining secure operations, supporting investigations of privacy breaches and responding to requests from consumers about accesses to their information that were mediated by the NHIE. These requests are described in Annex 7. Provide Consumer Access to Access and Disclosure Logs.

Great care must be taken that the logs themselves do not create disclosure risk.

### 5.3.2 Authentication (Person)

All participating systems shall authenticate the user that is the direct user of a system before permitting access to NHIN functions or data retrieved via the NHIN. Acceptable authentication strength will be determined in the future.

To be meaningful, user authentication depends on the organization that operates the authenticated system to do an effective job of proofing the identity of the users. In transactions to the NHIE, the user is identified without ambiguity and the user ID is identified with the organization providing the authentication. This attestation might be transitive, as described in this scenario:

- In building an NHIE, the Northern District HIE signs the necessary agreements to support health interchange with Memorial General Hospital.
- The process of establishing this business relationship is robust enough that the Northern District Health Information Exchange can say that it has verified the corporate identity of Memorial General Hospital and can attest to the fact that it is a legitimate hospital with reasonable policies, procedures and technological safeguards to ensure that its users are properly identified and authenticated.
- Memorial General Hospital grants attending privileges to Dr. Alfred Newby.
- Memorial General's credentialing and attending intake includes verifying (proofing) the identity of Dr. Newby and assigning the passwords, tokens or other means of authenticating Dr. Newby as a system user.
- Big Hospital Chain, Inc. operates a Long-Term Care (LTC) facility in the same city. Big Hospital Chain chooses to operate as a self-contained NHIE, meaning that its

procedures for proofing user identities and authenticating users directly meet the standards for being an NHIE.

- Dr. Newby makes a query about a patient that can be fulfilled by providing records from the LTC facility of Big Hospital Chain. The chain of trust that allows the LTC facility to provide the information is as follows: Big Hospital Chain trusts Northern District HIE because of its status as an NHIE; Northern District trusts Memorial General to vouch for Dr. Newby.

### **5.3.3 Authentication (System)**

The standards used for exchanging messages among systems participating in the NHIE shall include a means for verifying that the systems that send and receive information are the systems they claim to be.

### **5.3.4 Data Integrity Checking**

NHIEs may offer the capability to validate the contents of messages sent to and through the NHIE over and above technical protocols that ensure that the message was not changed. Such capabilities may validate that the contents of a message are suitable for its purpose. For example, an NHIE might validate that structured lab data it handles fully meets the interoperability specifications that apply.

### **5.3.5 Error Handling**

The standards used for exchanging messages among the systems participating in the NHIE shall ensure that robust and informative information is available in the event of errors.

### **5.3.6 HIPAA De-Identification**

For specific interchange capabilities, there must be a facility to remove personal identifying data to an extent compatible with HIPAA privacy standards. NHIEs may offer this service to assist participating systems that are not able to do it on their own. Contrast this with Pseudonymize and Re-Identify, Section 5.3.9.

### **5.3.7 Holding Messages**

When the NHIE will be supporting secondary uses of clinical data, it may offer a service to its members of accumulating individual transactions for subsequent delivery to or retrieval by secondary users.

### **5.3.8 Non-repudiation**

The standards used for exchanging messages shall ensure that the sender of such a message cannot reasonably deny that it was the source of the message. These standards shall also include a means to ensure that once a participating system has received a message it cannot reasonably deny that it has received the message.

### **5.3.9 Patient Summary Record Support**

A patient summary record is a collection of information about a patient that is oriented toward providing a clinician with a well-selected set of data relevant to the patient's care. Its importance stems from the fact that the total body of data about a patient that might be retrieved through the NHIN may be so overwhelming as to be a barrier to good clinical decision making. It is very

relevant to first-responder and other emergent situations as well as to many situations where the patient is being handed off from one provider to another.

It is not clear whether NHIEs will provide this function by assembling information from multiple sources, relying on summaries prepared in advance by providers, or a mixture of these approaches.

This report takes the view that the transaction sequences necessary to provide a patient summary upon request or to push a patient summary are not different from those used for retrieving or pushing other kinds of reports. (Although the transaction sequences are the same, the implementation of them may be very different for patient summary.)

Because there are no different transaction sequences, there is no annex for patient summary. Because different annexes represent the transaction sequences for pushing and pulling data, the patient summary record is listed as a common feature.

### **5.3.10 Pseudonymize and Re-Identify**

There must be a facility to remove the identifying portion of protected health information in a manner consistent with intended use. The term pseudonymize describes modifying personal health information to include disguised personal identification information such that (a) the identity of the subject is not immediately apparent; (b) the information content fits the needs of the use case; and (c) it is possible for the agent that modified the data, or its designee, to restore the identity information upon authorized request. The specific identifying information that is permissible to be retained in the clear is a matter of policy and may vary based on use case. For example, a policy determination for some use cases might support the requirement for fine-grained geographical data on otherwise disguised subjects.

The organization that pseudonymizes data must be able to re-associate that data with the identified patient upon receipt of an authorized request.

NHIEs may offer this service to assist participating systems that are not able to do it on their own. Contrast this with HIPAA De-Identification in Section 5.3.6.

### **5.3.11 Secure Transport**

The standards used for exchanging messages shall include a means for ensuring that transmissions between systems are delivered confidentially, reliably and intact.

### **5.3.12 Transmit Disambiguated Identities**

Messages that will be initiated because of the actions of users of a participating system shall contain sufficient information identifying the user such that it can be unambiguously traced to the user by the participating organization.

In support of this feature, NHIEs will need to establish schemes to unambiguously scope subject IDs.

The messages supporting actions that contain information about a patient shall, where practical, contain sufficient identifying information that the NHIE could match the patient with other patients being tracked by the NHIE or perform inter-NHIE subject adjudication.

It is possible that some of the identifying information transmitted about healthcare providers could include a subset of information that is collected as part of provider credentialing, in the sense of determining the professional qualifications of a provider to work in a specific healthcare setting.

## 5.4 Ensuring Authorization

Authorization is the granting of rights, which includes the granting of access, based on permissions. It is not listed as a common transaction feature, but it is nonetheless an important characteristic that ties together several features and transaction packages. This section brings the concepts together for discussion. Authorization cannot be reliably performed unless identity proofing and authentication has been performed on the user. See Section 5.3.2.

Information about a patient may reach various users (people or organizations) via the NHIN through various interchange capabilities as described in the annexes to this report. This information sharing can only happen consistent with the policies in place in each NHIE that is involved in a specific information flow. NHIEs may have different policies based on the preferences of participants in the NHIE and the laws or regulations of the specific jurisdictions in which the participants operate. This includes federal laws and regulations.

Ensuring compliance with specified policies on information flow requires several common capabilities as described below. Where this material describes the requirement of a participating organization that operates an EHR, PHR or other system, those requirements also apply to the NHIE itself, to the extent that it has direct users through a portal. Note that system authentication and user authentication are co-requisite capabilities which are both required, as illustrated in the steps below, to ensure that authorization is meaningful.

- Participating organizations will take responsibility for accurately confirming the identity of all persons who use systems that can send and receive information through an NHIE. They may take actions themselves to confirm identity or they may advisedly trust another organization for that. For example, a hospital may directly confirm the identity of users. It may participate in an HIE that relies on identifications made by the hospital. The HIE may participate in the NHIN through an NHIE which relies on the HIE.
- Participating organizations will authenticate each user that can send or receive information through the NHIE with a level of certainty at least as strong as that specified by the NHIE
- User IDs are not necessarily unique to a participating organization. Each NHIE will establish with its participants a manner of providing scope information so that a fully scoped user ID will be unique in the NHIN.
- Not all NHIEs will maintain a registry of users. No such registry is specified in this document. (They will have a registry of providers and be able to identify providers with one or more organizations' systems for routing, but the set of all registered providers is not the same as the set of all users.)
- Standards that enable information flows through NHIEs will support the transmission of the disambiguated user ID for all transactions performed on behalf of a user. They will also support the transmission of a disambiguated organization ID for all transactions.
- Standards will also support transmitting a description of the roles of users along with their disambiguated identities. This role information may include some level of information about the professional orientation of a user that is a provider.
- The systems of participating organizations that provide information in response to requests from the systems of other organizations may use the user and organizational identity and role information to enforce local restrictions on providing information.
- The NHIEs will maintain registries of the permissions that consumers give to organizations or providers to receive a consumer's data.

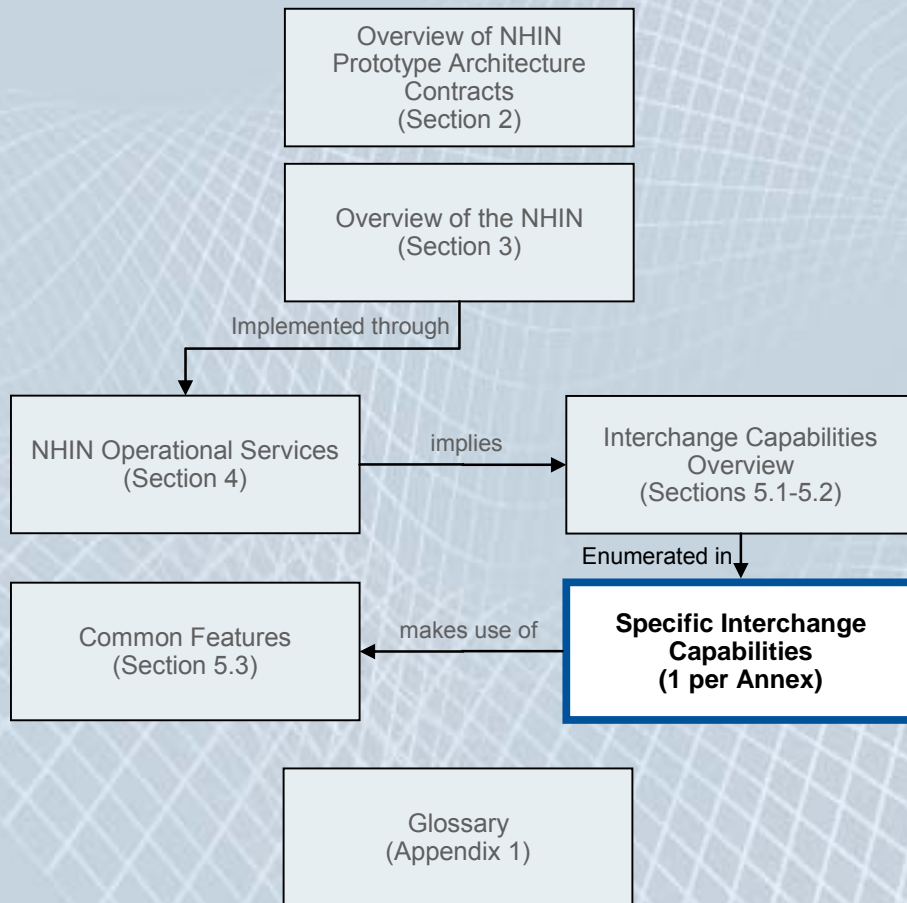
- An NHIE will support a declaration that the privileges of a provider to use the NHIN have been suspended.
- Consistent with policy determinations the NHIE will enforce the restrictions specified by consumer permissions or suspended privileges while passing transactions from one system to another.
- An NHIE will support the declaration of a need to override the restrictions that support consumer preferences in an emergent situation. This is referred to as a break-the-glass capability. When a break-the-glass situation has been declared, the NHIE will not interfere with the flow of information, although it will retain a complete audit trail of how information flowed. The implementation of break-the-glass functionality may be different in different NHIEs to account for differences in policy associated with their participants. Describing the requirement to use protocols that permit break-the-glass in this report is not meant to imply that the function must always be implemented in the same way, or at all. That is a policy issue.

## 5.5 Concluding Comments

The interchange capabilities and common features described in this final section of our report must be provided by the NHIEs in order to ensure that the NHIN functions reliably and securely. As described earlier, there is a many-to-many relationship between interchange capabilities described in the annexes and the common features.

The intent of this report is not to specify how those common features or interchange capabilities will be performed, but rather to describe and give a name to those areas based on the collective work of the NHIN prototype contractors. As the standards and policies required for enabling the NHIN evolve, these constructs will take shape and form the basis for the NHIN.

■ ■ ■ ■ **Annexes**



## Annexes

As described in Section 5.2, each of the numbered annexes that follow defines a specific set of interchange capabilities. This section contains an overview of the annexes, showing how each makes use of transaction packages from other annexes.

Note that the interchange capability described in an annex often shares the name of a transaction package that is defined within the annex. For example, the Identify Subject annex contains a transaction package called Identify Subject.

**Table 10. Annex Overview**

Annex	Uses Transaction Package	Description
<b>General</b>		
<b>Identify Subject</b>		Based on a query or the contents of a record, determine if an NHIE subject registry has a record that matches the subject referenced in the query or record.
	Identify Subject	Search for candidate subject matches from an NHIE registry
<b>Arbitrate Identity</b>		Request, assess, reconcile and link cross-registry candidate subject matches. An NHIE determines whether another NHIE, an EHR or PHR has a record that matches the subject referenced in a query or record. The NHIE reviews candidate matches from its own registry and that of the other system and applies algorithms to assess the likelihood of a match. After reconciling the candidate matches, the NHIE returns selected candidates in response to the query or, in the case of messages, determines if the message contents reliably identify a subject.
	Identify Subject	Search for candidate subject matches within an NHIE registry
	Arbitrate Identity	Request, assess, reconcile and link cross-registry candidate subject matches
<b>Locate Records</b>		Locate the records within an NHIE or among several NHIEs for a patient who has been identified by attributes.
	Identify Subject	Search for candidate patient matches within an NHIE registry based on the subject-identifying information provided by a user requesting the record location
	[Arbitrate Identity]	Request, assess, reconcile and link cross-registry candidate patient matches based on the subject-identifying information provided by a user requesting the record location
	Locate Records	Retrieve any available locations that have records for the identified patient, within an NHIE and possibly from several NHIEs

Annex	Uses Transaction Package	Description
<b>Retrieve Data</b>	Enable consumers and providers to view or access patient records within and across NHIEs.	
	Identify Subject	Search for candidate subject matches within an NHIE registry based on the subject-identifying information provided by user requesting data retrieval
	[Arbitrate Identity]	Request and assess cross-registry candidate subject matches based on the subject-identifying information provided by user requesting data retrieval
	Locate Records	Search within an NHIE and across NHIEs to identify the location of patient records based on location parameters specified by the user requesting data retrieval
	Retrieve Data	Provide the requested data from the identified record locations in response to the user request
<b>Route Data</b>	Some messages, e.g., lab results, have content that indicates the providers and CDOs that should receive copies. The NHIE reviews these contents and distributes the messages accordingly. The distribution may be within the NHIE or across NHIEs.	
	[Arbitrate Identity]	Request and assess cross-registry candidate subject matches based on the subject-identifying information included in the content of a message, e.g., lab result, prescription (this process is algorithmically different because the request does not originate with a user)
	Route Data	Forward the message to the appropriate location based on the identified patient and/or provider referenced in the message
<b>Consumer</b>		
<b>Publish PHR Location</b>	Identify where the consumer's PHR data are stored and publish the location as specified by the consumer.	
	Identify Subject	Search for candidate subject matches for the consumer within an NHIE registry
	[Arbitrate Identity]	Request and assess cross-registry candidate subject matches for the consumer
	Publish PHR Location	Based on the consumer's preferences, make known the location of the consumer's PHR record
<b>Maintain Consumer Data Sharing Permissions</b>	Consumers may identify providers that may view or access their PHR data. These permissions are shared with the NHIE so that they can be enforced by the NHIE in responding to data queries or when routing data.	
	Identify Subject	Search for candidate subject matches for the consumer within an NHIE registry
	[Arbitrate Identity]	Request and assess cross-registry candidate subject matches for the consumer
	Maintain Consumer Data Sharing Permissions	Register and maintain the consumer's permissions for allowing providers to view and access their data

Annex	Uses Transaction Package	Description
<b>Provide Consumer Access to Access and Disclosure Logs</b>		<p>The NHIE maintains audit logs of accesses to data and sharing of data. A consumer may request to review these records. The NHIE provides to the consumer's PHR copies of the access and disclosure data. These may be provided in response to a query from the consumer or they may be copied to the consumer's PHR as they are recorded at the NHIE.</p>
	Identify Subject [Arbitrate Identity]	<p>Search for candidate subject matches for the consumer within an NHIE registry</p> <p>Request and assess cross-registry candidate subject matches for the consumer</p>
	Provide Consumer Access to Access and Disclosure Logs	<p>Make available to the consumer NHIE records of accesses to and disclosures of their records</p>
<b>Route Consumer Request to Correct Data</b>		<p>The NHIE sends a consumer request for data correction to the system that is the source of the data. The source system or personnel responsible for the data must determine if there is an error in the data, amend the data if there is an error, and return the status of the request to the consumer's PHR.</p>
	Identify Subject [Arbitrate Identity]	<p>Search for candidate subject matches for the consumer within an NHIE registry</p> <p>Request and assess cross-registry candidate subject matches for the consumer</p>
	Locate Record	<p>Search within an NHIE and across NHIEs to identify the location of patient records based on location parameters specified by the consumer in his/her request for data correction</p>
	Route Consumer Request to Correct Data	<p>Send the consumer request for data correction to the system where the record is located. Return status to consumer's PHR.</p>
<b>Route Data Based on Consumer-Specified Preferences</b>		<p>Consumers may determine that specific providers should receive copies of all or selected updates to their medical information. Consumers can register these preferences with the NHIE. As the NHIE receives data, it compares the contents to consumer-registered preferences and forwards the data to the consumer-specified providers. This distribution is in addition to data distribution that is based on the contents of the data received, e.g., ordering provider for a lab result.</p>
	Identify Subject [Arbitrate Identity]	<p>Search for candidate subject matches for the consumer within an NHIE registry</p> <p>Request and assess cross-registry candidate subject matches for the consumer</p>
	[Locate Record]	<p>Search within an NHIE and across NHIEs to identify the location of patient records</p>
	Route Data Based on Consumer-Specified Preferences	<p>Send data to the PHR or EHR that the consumer has specified to receive the updates to his/her medical information</p>

Annex	Uses Transaction Package	Description
<b>Secondary Use</b>		
<b>Manage Data Selection Parameters for Secondary Use</b>	Secondary users, such as Public Health and Data Quality organizations, have filtering or data selection criteria for identifying data of interest. These parameters are sent to the NHIE. The NHIE forwards the parameters to the appropriate source systems. The source systems use the parameters to screen records and identify those that should be forwarded to the NHIE for distribution to secondary users. The criteria could also be used to formulate queries from the NHIE to PHRs and EHRs to obtain the data.	Manage Data Selection Parameters for Secondary Use      Forward new and updated data selection parameters to appropriate source systems
<b>Pseudonymize and Re-Identify Data</b>	The NHIE removes identifying information from records before they are sent to secondary users (if this has not already been done by the source system). In some instances it will be necessary, with appropriate authorization, to re-identify a pseudonymized record, e.g., to enable public health officials to contact an individual with a communicable disease. With proper controls, the NHIE will re-identify a record or request re-identification from the source system. Note: in many instances the operational service of pseudonymizing and re-identifying data will be provided directly by the organization sending the data rather than by the NHIE.	Pseudonymize and Re-Identify Data      Remove identifiers from patient records. The NHIE maintains a mechanism to re-associate the data with the patient.
<b>Provide Data to Secondary Users</b>	Source systems such as EHRs and PHRs will utilize data filtering or data selection parameters to identify records of interest to secondary users, or NHIEs may request data via a query that incorporates the data selection parameters. These records will be forwarded to the NHIE. The NHIE will identify the secondary users that should receive the records and forward them directly or through other NHIEs.	[Pseudonymize and Re-Identify Data]      The NHIE removes identifying information from records before they are sent to secondary users (if this has not already been done by the source system)  Provide Data to Secondary Users      Receive records for secondary use from source systems and forward them to the appropriate secondary users
<b>Management</b>		
<b>Maintain Registries of NHIN-Participating Systems and Organizations</b>	NHIEs register and update information on organizations/systems authorized for access to and from the NHIN. The NHIE associates its own identifier with each organization/system. The registry includes specifications of the type of access allowed, organization demographics, contacts and messages supported. The NHIE propagates the organization and system registrations to all other NHIEs within the NHIN.	Maintain Directories of NHIN-Participating Systems and Entities      Create and maintain registration records for systems and entities associated with the NHIE

## Annex 1. Arbitrate Identity

### *Description*

Request, assess, reconcile and link cross-registry candidate subject matches.

Arbitration of subject identities is a process that occurs on an as-needed basis when two or more participants in a transaction may each have lists of candidates that must be reconciled to a specific set of identifying data. It is distinct from the process described in Identify Subjects because it involves the simultaneous use of two identity registries. The NHIE may be seeking to reconcile its own registry with the registry of a CDO, of another NHIE, or among the NHIE's internal registries (if the NHIE has multiple patient or provider registries).

In order to share patient data within and among NHIEs, and at times between NHIEs and connected organizations, it is necessary to have mechanisms to match patient and provider identities in the absence of a single national identifier. Even where an identifier may exist, there is a need for identifying common patients or providers, because existing systems may not have adapted to the identifiers, or identifiers are not fully synchronized.

Each NHIE maintains its own internal patient and provider registries. When an NHIE cannot identify a subject from its patient or provider registry or a cross-NHIE query is made, the requesting NHIE must send patient and/or provider data that can be used by the responding PHR/EHR or NHIE to determine if there is a record for the specified patient or provider in its registry. The responding PHR/EHR or NHIE sends the requesting NHIE any candidate matches. The requesting NHIE uses this information along with its own patient or provider registry to determine if any of the candidates may be a match. The requesting NHIE may rule out some of the candidate records and forward any remaining candidate records to the user or system originating the query. The user can indicate if any of the candidate records are a match. The review of candidate records may require human intervention or may be automated. The results of the record selection are returned to the requesting NHIE and forwarded to the responding NHIE.

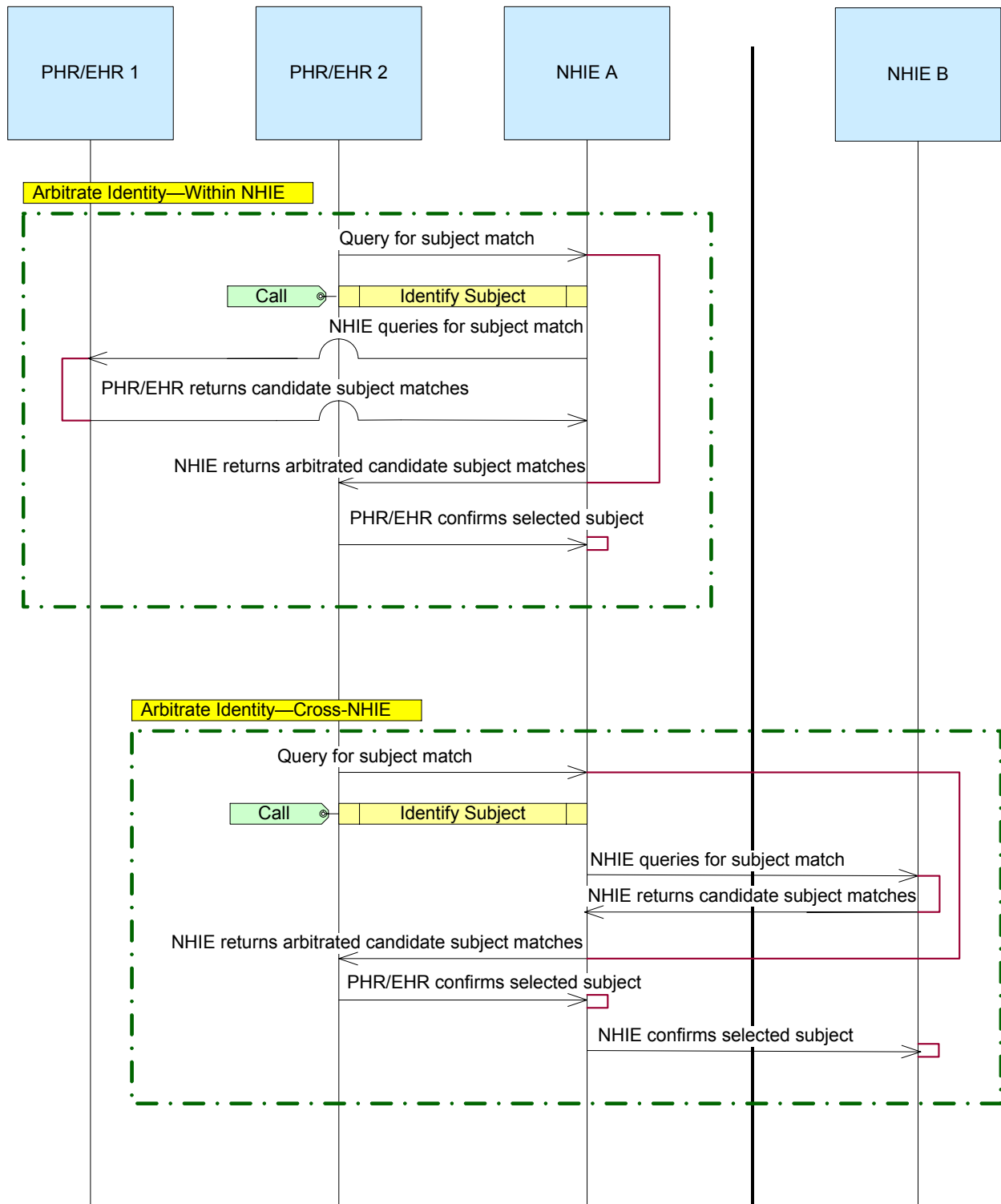
### *Illustrative Example*

Mr. David Jefferson spends winters in Texas and summers in Idaho. While in Texas, Mr. Jefferson visits an emergency department complaining of chest pains. He informs the ED personnel that he is regularly seen by Dr. Brown in another town in Texas and by Dr. Williams in Idaho. In Idaho he was treated in the Community Medical Center for chest pains last summer. Dr. Brown's practice participates in the same HIE as the ED in Texas. Dr. Williams and Community Medical Center both participate in the same HIE in Idaho.

The ED physician determines that specific findings and EKG data from Mr. Jefferson's prior encounters would be important in evaluating his condition. The Texas HIE has several David Jeffersons but has been able to recognize that two patient entries for David Jefferson represent the same patient, with slight variations on the spelling. On behalf of the EHR at the ED, the Texas HIE receives possible matches from the Idaho HIE and is able to positively match identity to a David Jefferson who was treated at the Community Medical Center and Dr. Williams.

Using the arbitrated identity data the Texas HIE retrieves specific information as described in another annex.

### Diagram



## **Transactions**

### **Arbitrate Identity—Within NHIE**

Query for subject match—A PHR or EHR provides subject demographic data or other attributes and requests NHIE A to identify matching records, or NHIE A is routing a record with subject-identifying information.

NHIE A queries for subject match—NHIE A is unable to identify the subject based on records in the NHIE A's patient or provider registry. NHIE A forwards the subject's demographic information to a PHR/EHR, requesting any matching records.

PHR/EHR returns candidate subject matches—the responding PHR/EHR reviews its master patient or provider index and identifies any records that may be a match.

NHIE A returns arbitrated candidate subject matches—NHIE A reviews the records returned from the PHR/EHR and determines those that should be returned to the requestor as possible matches.

PHR/EHR confirms selected subject—The PHR/EHR user reviews the candidate matches and indicates if any are determined to be a match.

### **Arbitrate Identity—Across NHIE**

Query for subject match—A PHR or EHR provides subject demographic data or other attributes and requests NHIE A to identify matching records from other NHIEs, or the NHIE is routing a record with subject-identifying information.

NHIE A queries for subject match—NHIE A forwards the subject's demographic information or other attributes to NHIE B, requesting any matching records.

NHIE B returns candidate subject matches—The NHIE B reviews its patient or provider registry and identifies any records that may be a match.

NHIE A returns arbitrated candidate subject matches—The NHIE A reviews the records and determines those that should be returned to the requestor as possible matches.

PHR/EHR confirms selected subject—The PHR/EHR user reviews the candidate matches and indicates if any are determined to be a match.

NHIE A confirms selected subject—The NHIE A informs the NHIE B of the outcome of the match determination.

***Common Features of Transactions***

<b>Feature</b>	<b>Feature Applicability</b>
Audit Logging	X
Authentication (Person)	X
Authentication (System)	X
Data Integrity Checking	X
Error Handling	X
HIPAA De-Identification	
Holding Messages	
Non-repudiation	X
Patient Summary	
Pseudonymize and Re-Identify	
Secure Transport	X
Transmit Disambiguated Identities	X

***Logical Registries Referenced by Transactions***

<b>Registry</b>	<b>Used</b>
Consumer	X
Patient	X
Provider	X
PHR Record Location	X
EHR Record Location	X
Consumer Permissions	
Consumer Data Sharing Preferences	
Organizational Participant	X
System/Network	X

## Annex 2. Identify Subject

### *Description*

Based on a query or contents of a record, determine if an NHIE subject registry has a record that matches the subject referenced in the query or record.

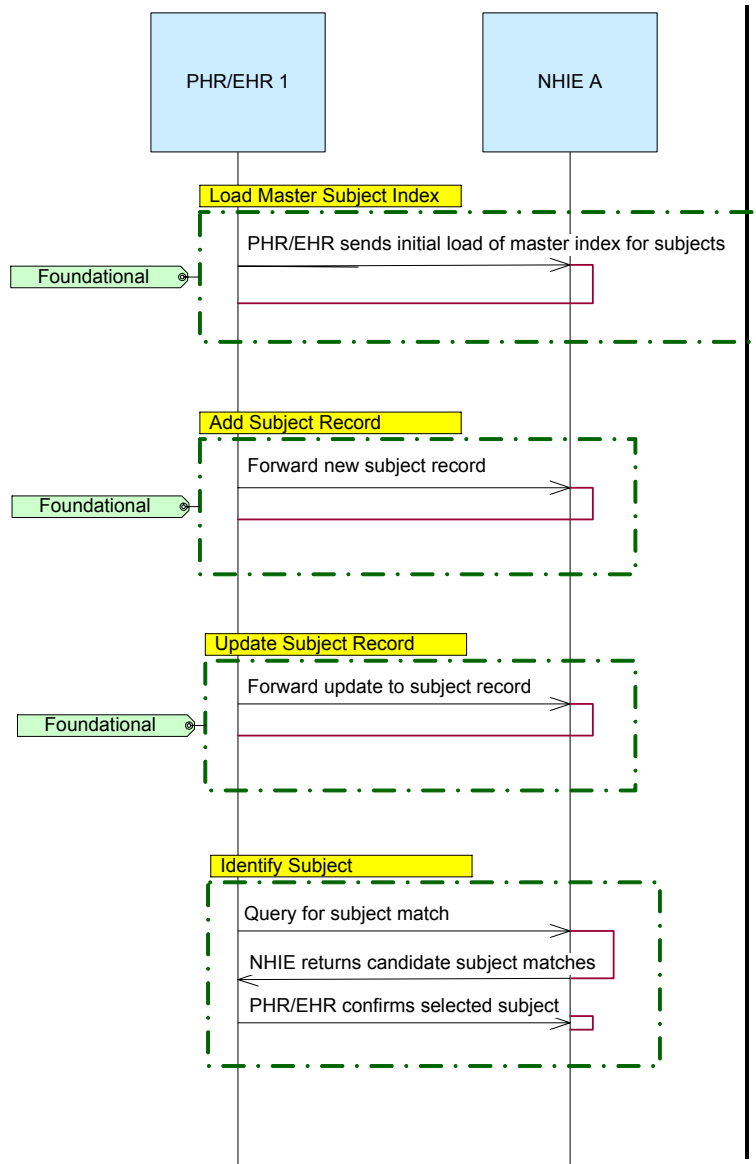
Patients and providers may have records identifying them in more than one system participating in an NHIE. In order to perform certain operations, including responding to queries or directing data to the appropriate system, the NHIE must have a mechanism for identifying patients and providers. As new systems join the NHIE, they may provide a copy of their master patient indexes for patients and providers. The NHIE incorporates these master indexes into its own registry that can be used as a reference for identifying the patient, or provider associated with a query or data transaction. (The automated load may identify records that must be resolved by the sending system before they can be loaded in the NHIE Registry. This will require manual review and resolution between the sending organization and the NHIE.) As queries or transactions are received from PHRs, EHRs and other NHIEs, the NHIE reviews its patient or provider registry and applies algorithms to identify possible matching subject records. NHIEs may use different matching algorithms to support different requirements. The candidate subject matches are returned to the source of the query. When a matching record is selected by the query originator (the selection of the subject match may be done by the user or automated), the NHIE is notified of the selected subject match. The NHIE can use this information to refine future subject matching.

The NHIE may also use its provider registry to enforce data access controls. Provider records would include information, such as, specialty or type of practice that the NHIE could use to determine if data should be routed to a provider, or if the NHIE should retrieve data in response to a provider's query. In instances where a provider is suspended from NHIE access, the provider registry could be used to indicate that the provider's no longer has access to the NHIE.

### *Illustrative Example*

Dr. Jones is a member of a group practice that has an EHR system that participates in an NHIE. In order to have better access to its patients' data, Dr. Smith's group has decided to participate in the same NHIE. When Dr. Smith's practice signed up with the NHIE, it provided a copy of its EHR's master index for patients and providers. These were loaded into the NHIE's master patient and provider registries. Dr. Jones has a new patient, Miss Wilson. Miss Wilson is registered in the EHR for Dr. Smith's practice. The EHR system sends a copy of the new registration to the NHIE, where it is integrated into the patient registry. The next time Miss Wilson comes to Dr. Smith's office, she indicates that she has moved and her address is updated in the EHR. A copy of the updated information for Miss Wilson is sent to the NHIE to update its patient registry. On Miss Wilson's next visit, she informs Dr. Smith that she has records at a hospital that also participates in the local NHIE. Dr. Smith makes an inquiry through the NHIE to obtain a copy of these records. As a first step in locating these records, the NHIE reviews its patient registry to identify those that might be a match for Miss Wilson. The NHIE finds two possible matches that have identical information but different addresses. Both matches are displayed to Dr. Smith who notices that the records are different. Dr. Smith confirms the correct record with Miss Wilson. He selects this record and indicates that the NHIE should search using this patient. According to its policy the NHIE uses Dr. Smith's matching confirmation to update its patient registry.

**Diagram**



## Transactions

### Load Master Subject Index

PHR/EHR sends initial load of master patient or provider indexes. As new systems join NHIE A, they provide their master indexes of patients and providers. NHIE A incorporates these records into its patient and provider registries.

### Add Subject Record

Forward new subject record—Systems participating in NHIE A forward copies of new patient and provider records to NHIE A. These records are added to NHIE A's patient or provider registry.

### Update Subject Record

Forward update to subject record—Systems participating in NHIE A forward copies of updates to patient and provider records to NHIE A. These updates are incorporated into NHIE A's patient or provider registry. Updates may include merges, unmerges, deletions and suspensions.

### Identify Subject

Query for subject match—A source system makes a request to NHIE A that requires that the appropriate patient or provider be identified from the NHIE A's registry.

NHIE A returns candidate subject matches—NHIE A sends the requestor any candidate-matching patient or provider records. NHIE A may notify the requestor that there are no matching records or send several candidate-matching records.

PHR/EHR confirms selected subject—If one or more possible matches are returned to the requestor, the requestor selects, confirms or declines the candidate match and notifies NHIE A of the determination. (The selection of a matching record may be done by a user or automated, according to policy.)

## Common Features of Transactions

Feature	Feature Applicability
Audit Logging	X
Authentication (Person)	X
Authentication (System)	X
Data Integrity Checking	X
Error Handling	X
HIPAA De-Identification	
Holding Messages	
Non-repudiation	X
Patient Summary	
Pseudonymize and Re-Identify	
Secure Transport	X
Transmit Disambiguated Identities	X

***Logical Registries Referenced by Transactions***

<b>Registry</b>	<b>Used</b>
Consumer	X
Patient	X
Provider	X
PHR Record Location	
EHR Record Location	
Consumer Permissions	
Consumer Data Sharing Preferences	
Organizational Participant	X
System/Network	X

## Annex 3. Locate Records

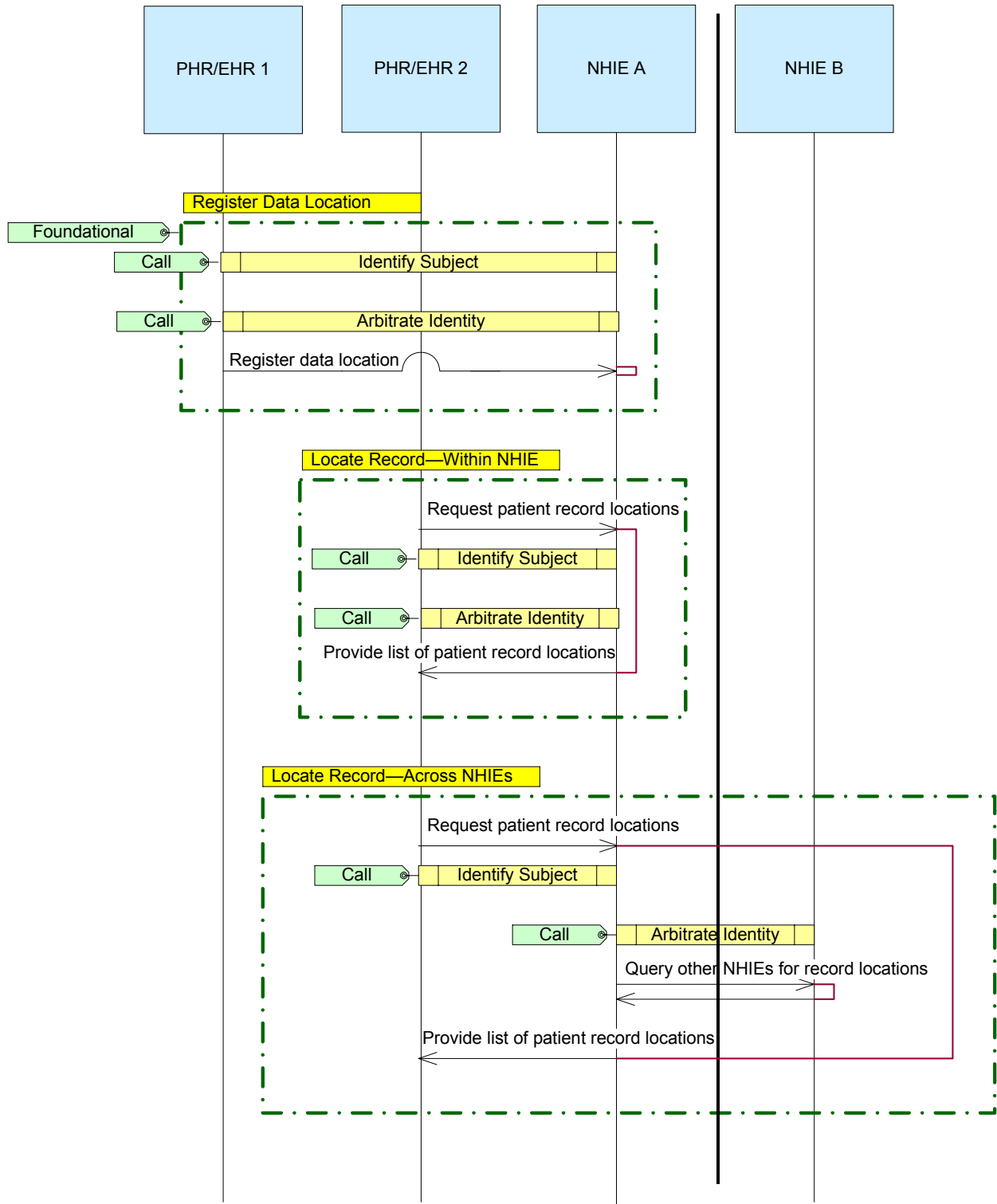
### *Description*

Locates the records within an NHIE or among several NHIEs for a patient who has been identified by attributes because there is no national identifier. Stores the location of patient records and provides users with information on where patient records are located. Record location information can also be used by the NHIE to assist in routing data such as lab results and medication information.

### *Illustrative Example*

Mrs. Phillips is admitted to the hospital for hip replacement surgery. At the time of admission, the hospital EHR notifies the local NHIE that Mrs. Phillips has a record in the hospital's system. After being discharged from the hospital Mrs. Phillips has a routine visit with her gerontologist, Dr. Caine. Mrs. Phillips mentions her hip replacement surgery to Dr. Caine. Dr. Caine uses his EHR to request Mrs. Phillips' records from the hospital. The NHIE searches its record location information and determines that a record is available for Mrs. Phillips at the hospital where she had her surgery. Dr. Caine requests the records on Mrs. Phillips' hip replacement surgery. During the visit, Mrs. Phillips mentions that she had been treated for breathing difficulty by Dr. Porter while she was traveling in Texas. Dr. Caine makes another request to the NHIE to locate records for Mrs. Phillips in Texas. The local NHIE makes a request to the NHIE supporting Texas to determine if there are any records for Mrs. Phillips. The Texas NHIE sends a response indicating that there are records for Mrs. Phillips at the practice with which Dr. Porter is associated. Dr. Caine requests the NHIE to retrieve Mrs. Phillips' records from the Texas NHIE.

### Diagram



## Transactions

### Register Data Location

Register data location—As patients receive care for the first time from a provider, EHR 1 notifies NHIE A that there is a record for the patient at the provider's location.

### Locate Record—Within NHIE

Request patient record locations—PHR/EHR 2 queries NHIE A for patient record locations within NHIE A's affiliated systems.

Provide list of patient record locations—After reviewing the record location data, NHIE A returns the list of locations that match the PHR/EHR 2 user's request.

### Locate Record—Across NHIEs

Request patient record locations—PHR/EHR 2 queries the NHIE A for patient record locations within NHIE B's affiliated systems.

Query other NHIEs for record locations—NHIE A requests NHIE B to determine if there are records for the identified patient in its affiliated systems. The NHIE B returns a list of any record locations for the patient.

Provide list of patient record locations—NHIE A forwards the responses from NHIE B to the PHR/EHR 2 making the record location request.

## Common Features of Transactions

Feature	Feature Applicability
Audit Logging	X
Authentication (Person)	X
Authentication (System)	X
Data Integrity Checking	X
Error Handling	X
HIPAA De-Identification	
Holding Messages	
Non-repudiation	X
Patient Summary	
Pseudonymize and Re-Identify	
Secure Transport	X
Transmit Disambiguated Identities	X

**Logical Registries Referenced by Transactions**

Registry	Used
Consumer	X
Patient	X
Provider	X
PHR Record Location	X
EHR Record Location	X
Consumer Permissions	
Consumer Data Sharing Preferences	
Organizational Participant	X
System/Network	X

## Annex 4. Maintain Consumer Data Sharing Permissions

### *Description*

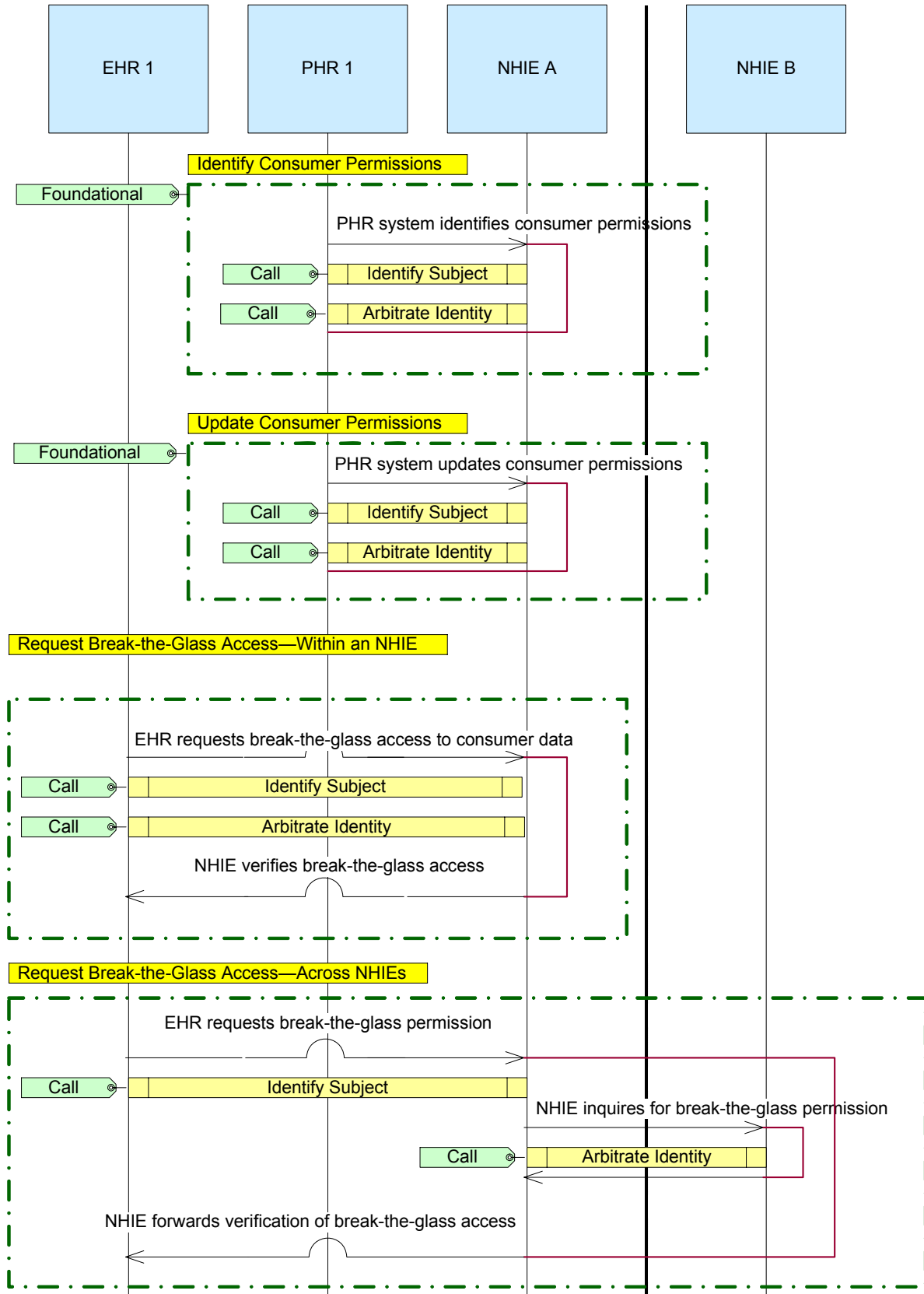
Consumers may choose to limit the providers that may view the records within their PHRs. Policy may dictate that they also be able to limit the type of data that may be available to any or selected providers. Policy may also dictate that consumer permissions be applied by the NHIE to the routing of data that does not come from the consumer's PHR.

Permission management tracks the consumer's permissions and applies them as data queries are received and, as required by policy, when data is routed through the NHIE. The NHIE will create and update consumer permissions and check all queries and data routing against the consumer's specified permissions. In emergency situations, the NHIE will authorize providers to override consumer restrictions on access for individual patients or for a population of patients.

### *Illustrative Example*

Sean has created a PHR and also utilizes several providers with EHRs. In addition to creating a PHR, Sean specified the providers who could access his records and the data that he wanted to allow the provider to access. Tomorrow Sean has a visit with an orthopedist for the first time. He accesses his PHR and requests to update his permissions. As he reviews his current permission profile he realizes that he has changed primary care providers and should remove his old provider and add his new primary care physician. Sean adds the new primary care physician and grants this provider access to all of his records. He also adds his new orthopedist and grants access only to records related to his leg injury. Later in the day, the orthopedist EHR queries the NHIE to obtain Sean's record for his visit tomorrow. The NHIE confirms that the orthopedist has permission to obtain Sean's records. The NHIE determines that Sean has restricted the orthopedist's access to selected medical information. The NHIE returns only the medical information that Sean has authorized the orthopedist to receive. The following week Sean is involved in a car accident that renders him unconscious. When he arrives at the emergency department, the staff is able to identify Sean from his driver's license. They log into the NHIE and request his medical records. The NHIE notifies the ED that they have not been granted access to Sean's records. The ED staff request the NHIE to allow them break-the-glass access to Sean's records. The NHIE recognizes the ED as a user with break-the-glass privileges and provides access to Sean's medical records.

### Diagram



## **Transactions**

### **Identify Consumer Permissions**

PHR 1 identifies consumer permissions—To record a consumer's decision to participate in the NHIN, PHR 1 registers the consumer's preferences for who can access their data and the data they want to allow each provider or surrogate to be able to access.

### **Update Consumer Permissions**

PHR 1 updates consumer permissions—As consumers change providers or have new preferences regarding the use of their data, updates to the consumers' permission profiles will be made.

### **Request Break-the-Glass Access—Within an NHIE**

EHR 1 requests break-the-glass access to consumer records—EHR 1 requires emergency access to the consumer's records, but is not included in the consumer's permission profile. EHR 1 asks NHIE A to override the permission profile and allow access to the consumer's medical information.

NHIE A inquires for break-the-glass permission—NHIE A reviews forwards the break-the-glass permission request and verifies that the requestor is authorized to override consumer permissions.

NHIE A verifies break-the-glass access—NHIE A notifies EHR 1 that break-the-glass permission to access the consumer's medical records has been verified.

### **Request Break-the-Glass Access—Across NHIEs**

EHR 1 requests break-the-glass access to consumer records—EHR 1 requires emergency access to the consumer's records within NHIE B, but is not included in the consumer's permission profile. EHR 1 asks NHIE A to request NHIE B to override the consumer's permission profile and allow access to the consumer's medical information.

NHIE A inquires for break-the-glass access—NHIE A requests NHIE B to grant break-the-glass access to EHR 1. NHIE B notifies NHIE A that it has granted break-the-glass access to EHR 1.

NHIE A forwards verification of break-the-glass access—NHIE A notifies EHR 1 that break-the-glass permission to access the consumer's medical records has been verified by NHIE B.

***Common Features of Transactions***

<b>Feature</b>	<b>Feature Applicability</b>
Audit Logging	X
Authentication (Person)	X
Authentication (System)	X
Data Integrity Checking	X
Error Handling	X
HIPAA De-Identification	
Holding Messages	
Non-repudiation	X
Patient Summary	
Pseudonymize and Re-Identify	
Secure Transport	X
Transmit Disambiguated Identities	X

***Logical Registries Referenced by Transactions***

<b>Registry</b>	<b>Used</b>
Consumer	
Patient	
Provider	X
PHR Record Location	
EHR Record Location	
Consumer Permissions	
Consumer Data Sharing Preferences	
Organizational Participant	X
System/Network	X

## Annex 5. Maintain Registries of NHIN-Participating Systems and Organizations

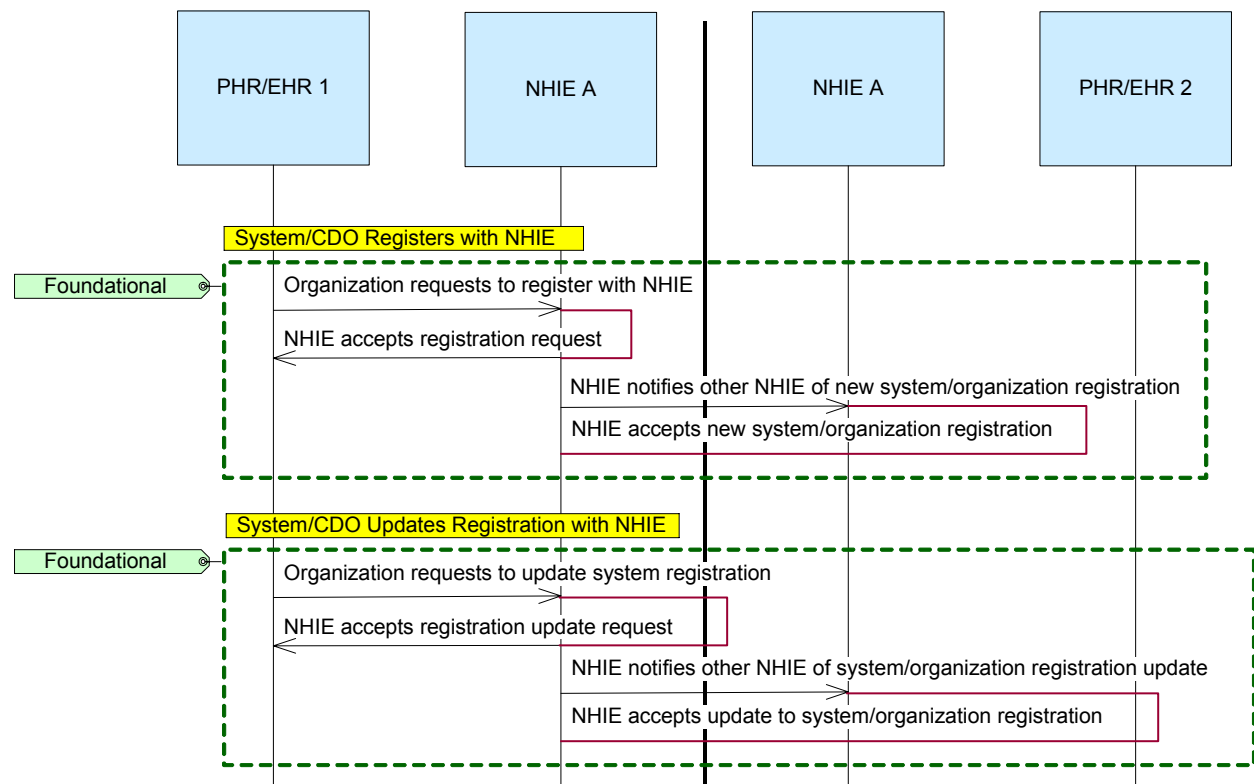
### Description

The NHIE will maintain information on each organization, network and system that participates in its information exchange. As new organizations, networks and systems agree to participate in an NHIE, the NHIE will add its information to its registry of organizations and systems. Data on organizations and systems also will be updated. These records may include: the type of access allowed, entity demographics, contacts, messages supported, capabilities and services. The NHIE will propagate the system or organization registration and updates to all other NHIEs within the NHIN. The NHIEs will use this information to support data routing and to identify NHIEs to query when the query includes CDO or system information.

### Illustrative Example

The Municipal General Hospital has established an agreement with the state NHIE to participate in the NHIN. After signing the agreement, the Municipal General Hospital provides registration data for the hospital as an organization on its inpatient EHR and other clinical systems that will interact with the state NHIE. After submitting the information, the NHIE staff reviews the registration data and confirms that the registration is complete. Once the registration is approved, the NHIE notifies other NHIEs that Municipal General Hospital is participating in the NHIN and is associated with the state NHIE. When Municipal General later implements a new ambulatory EHR that will also access the NHIE, Municipal General submits updated the system registration information. The NHIE forwards the update to other NHIEs.

### Diagram



## Transactions

### System/CDO Registers with NHIE

Organization requests to register with NHIE A—An organization provides registration information to NHIE A for itself, its network or some of its systems.

NHIE A accepts registration request—NHIE A reviews the registration data and creates a new organization, network or system record.

NHIE A notifies other NHIE B of new system/organization registration—NHIE A routes copies of appropriate parts of the system, network or organization registration data to NHIE B. (The data routed to other NHIEs may be a subset of the data maintained by the originating NHIE.)

NHIE B accepts new system/organization registration—The NHIE B confirms that the new registration has been added.

### System/CDO Updates Registration with NHIE

System/CDO requests to update registration—An organization provides updated registration information to NHIE A for itself, its network or some of its systems.

NHIE A accepts registration update request—NHIE A reviews the updated registration data and updates the organization, network or system registration record.

NHIE A notifies NHIE B of system/CDO registration update—NHIE A routes copies of appropriate parts of the system, network or organization registration data to NHIE B. (The data routed to other NHIEs may be a subset of the data maintained by the NHIE.)

NHIE B accepts update to system/organization registration—NHIE B confirms that the update to the registration has been made.

## Common Features of Transactions

Feature	Feature Applicability
Audit Logging	X
Authentication (Person)	X
Authentication (System)	X
Data Integrity Checking	X
Error Handling	X
HIPAA De-Identification	
Holding Messages	
Non-repudiation	X
Patient Summary	
Pseudonymize and Re-Identify	
Secure Transport	X
Transmit Disambiguated Identities	X

**Logical Registries Referenced by Transactions**

Registry	Used
Consumer	
Patient	
Provider	X
PHR Record Location	
EHR Record Location	
Consumer Permissions	
Consumer Data Sharing Preferences	
Organizational Participant	X
System/Network	X

## Annex 6. Manage Data Selection Parameters for Secondary Use

### *Description*

Secondary users, such as Public Health and Data Quality organizations, have filtering criteria for identifying data of interest. These parameters are sent to the NHIE. The NHIE forwards the parameters to the appropriate source systems. The source systems use the parameters to screen records and identify those that should be forwarded to the NHIE for distribution to secondary users. In instances where NHIEs maintain data repositories, the NHIE may use the parameters to screen and forward records in the NHIE's repository.

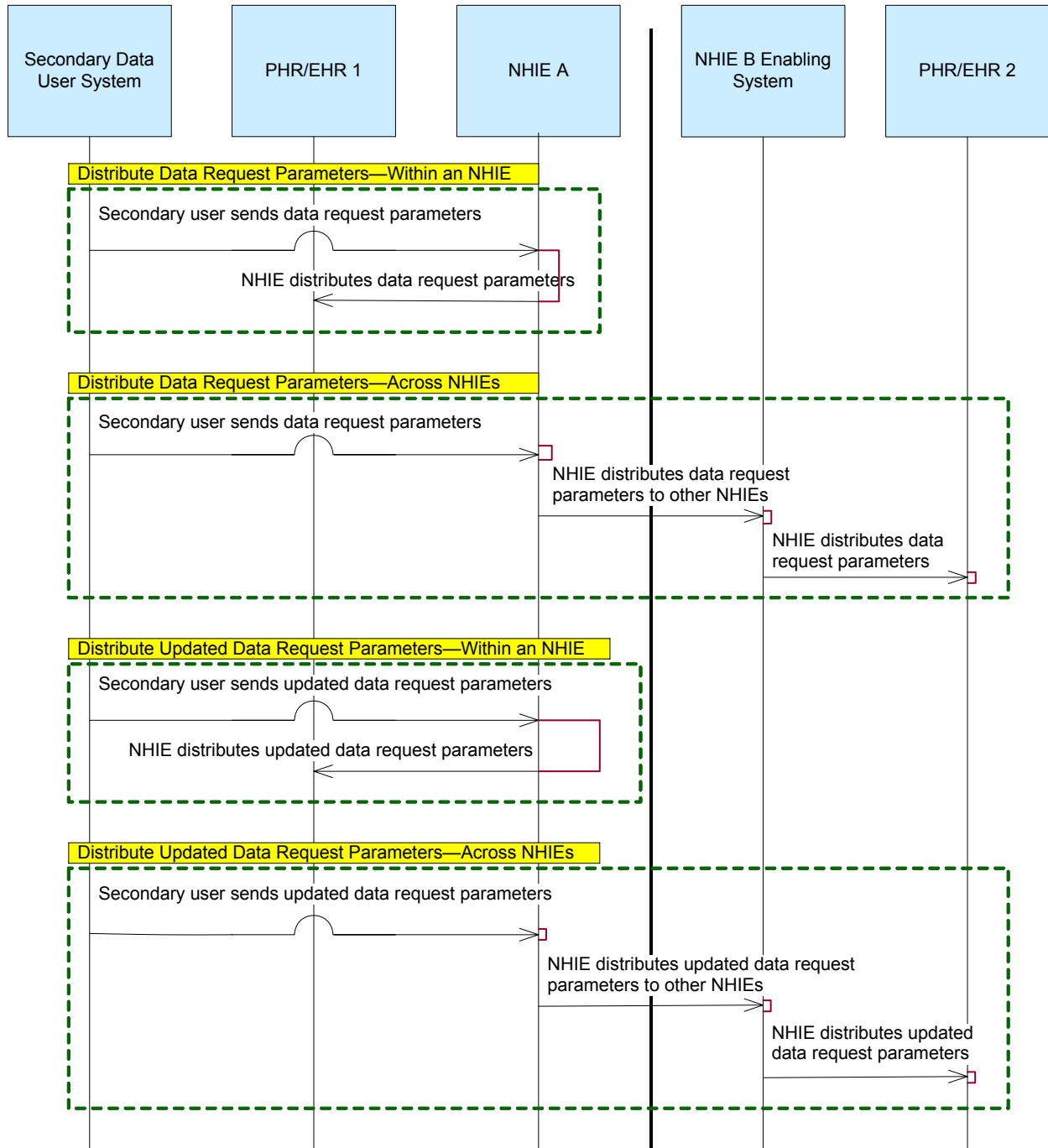
Note: The automated transmission of parameters modeled here applies to parameters within a well-defined range of variations, as determined by subsequent standards efforts. Outside of that range of parameters it will not be possible to distribute changes on an automatic basis.

This annex is silent on the manner in which the parameters are applied. It may subsequently be determined that the parameters primarily change filters so that the modified parameters only apply to future transactions. On the other hand, it may be that the changed parameters could be used for retrievals from repositories, allowing the new parameters to be applied retrospectively.

### *Illustrative Example*

A quality-monitoring organization measures the percentage of school-age children who are fully immunized. The quality-monitoring organization develops data selection specifications to be used by EHRs and PHRs to submit immunization data for use in the immunization measure. These specifications are sent to the NHIE for distribution to EHR and PHR systems that provide data to the quality-monitoring organization. The NHIE forwards the specifications to the appropriate EHRs and PHRs. As the quality-monitoring organization gains experience with the data for the immunization measure, refinements to the data selection criteria are specified. The quality-monitoring organization sends the specification updates to the NHIE. The NHIE forwards the revised specifications to EHR and PHR systems that provide data to the quality-monitoring organization.

### Diagram



## **Transactions**

### **Distribute Data Request Parameters—Within an NHIE**

Secondary user sends data request parameters—A secondary user sends data selection and filtering rules to NHIE A. NHIE A distributes data request parameters—NHIE A forwards the data request parameters to the EHR/PHR 1 that will provide data to the secondary user.

### **Distribute Data Request Parameters—Across NHIEs**

Secondary user sends data request parameters—A secondary user sends data selection and filtering rules to NHIE A.

NHIE A distributes data request parameters to NHIE B.

NHIE B distributes data request parameters—NHIE B forwards the data request parameters to PHR/EHR 2 that will provide data to the secondary user.

### **Distribute Updated Data Request Parameters—Within an NHIE**

Secondary user sends updated data request parameters—A secondary user sends changes to data selection and filtering rules to NHIE A.

NHIE A distributes updated data request parameters—NHIE A forwards the updated data request parameters to PHR/EHR 1 that will provide data to the secondary user.

### **Distribute Updated Data Request Parameters—Across NHIEs**

Secondary user sends updated data request parameters—A secondary user sends changes to data selection and filtering rules to NHIE A.

NHIE A distributes updated data request parameters to NHIE B—NHIE A forwards the updated data request parameters to NHIE B.

NHIE B distributes data request parameters—NHIE B forwards the updated data request parameters to PHR/EHR 2 that will provide data to the secondary user.

***Common Features of Transactions***

Feature	Feature Applicability
Audit Logging	X
Authentication (Person)	X
Authentication (System)	X
Data Integrity Checking	X
Error Handling	X
HIPAA De-Identification	
Holding Messages	
Non-repudiation	X
Patient Summary	
Pseudonymize and Re-Identify	
Secure Transport	X
Transmit Disambiguated Identities	X

***Logical Registries Referenced by Transactions***

Registry	Used
Consumer	
Patient	
Provider	
PHR Record Location	
EHR Record Location	
Consumer Permissions	
Consumer Data Sharing Preferences	
Organizational Participant	X
System/Network	X

## **Annex 7. Provide Consumer Access to Access and Disclosure Logs**

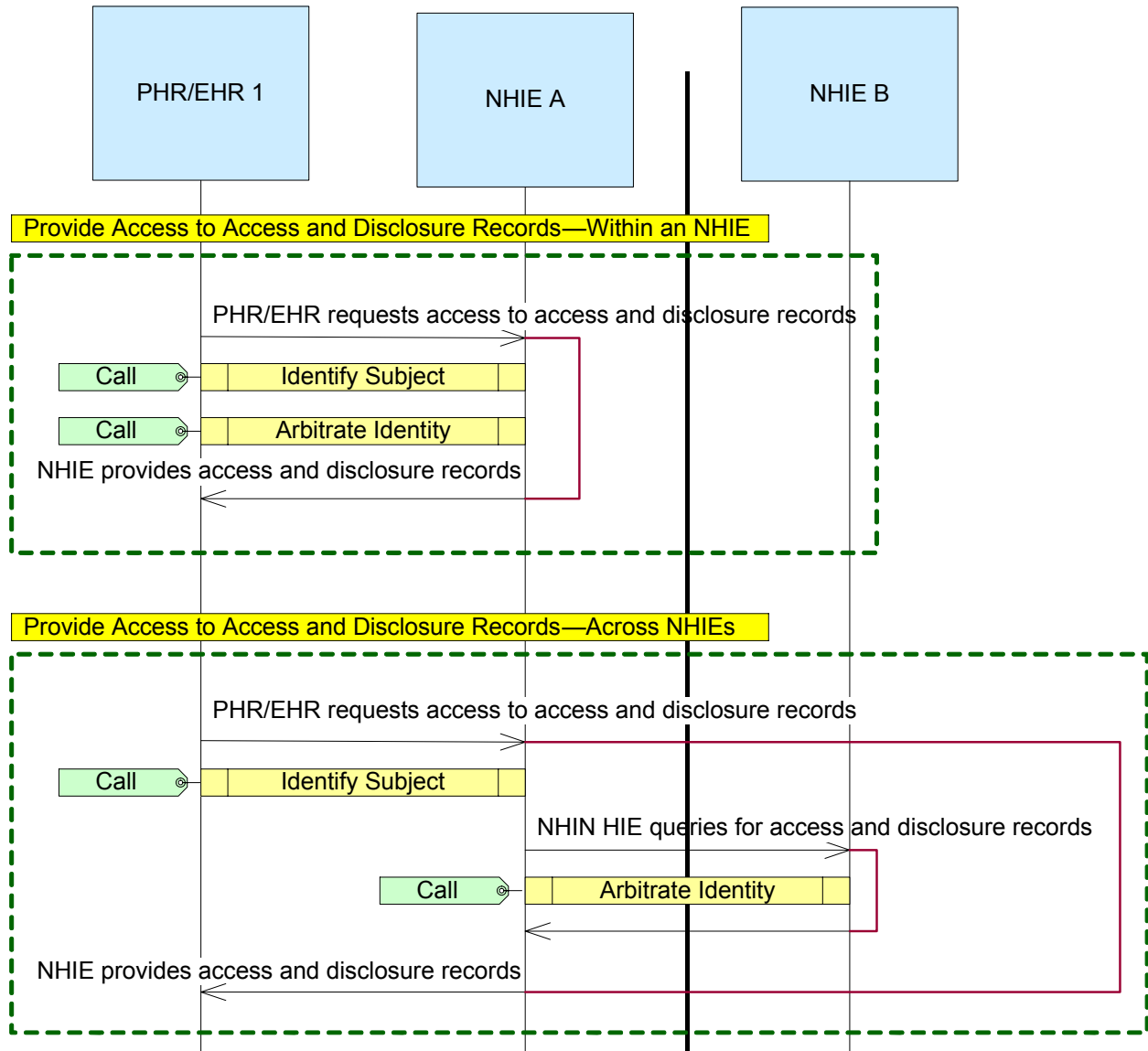
### ***Description***

Allows the consumer to retrieve records of accesses and disclosures of their data that were processed through an NHIE. Access and disclosure logs are records kept by the NHIE to provide an audit trail of data queries, updates and disclosures.

### ***Illustrative Example***

Peter Smith provided permission for his medical data to be shared via the NHIE. It is now one year after Peter signed up and he would like to know which data have been accessed or disclosed using NHIE services. Peter logs in to his PHR and asks to view the access and disclosures of his data that occurred within the NHIE. Because Peter lives in Florida in the winter and Maine in the summer, his data are processed through two different NHIEs. Peter's PHR sends a request for access and disclosure records to the NHIE to which the PHR is linked. The NHIE queries its own records and other NHIEs to find access and disclosure records for Peter. The other NHIEs return the access and disclosure records to the requesting NHIE, where the records are forwarded to Peter's PHR. The PHR provides Peter with a display of his access and disclosure records for review.

**Diagram**



## Transactions

### Provide Access to Access and Disclosure Records—Within an NHIE

PHR/EHR 1 requests access to access and disclosure records—A consumer requests to view access to and disclosures of their medical data that have been processed by NHIE A.

NHIE A provides access and disclosure records—NHIE A searches its access and disclosure records and forwards events associated with the requesting consumer to PHR/EHR 1.

### Provide Access to Access and Disclosure Records—Across NHIEs

PHR/EHR 1 requests access to access and disclosure records—A consumer requests to view access and disclosures of their medical data that have been processed by NHIE B.

NHIE A queries for audit events—NHIE A requests and receives access and disclosure records for the consumer from NHIE B.

NHIE A provides access and disclosure records—NHIE A forwards access and disclosure records to PHR/EHR 1.

## Common Features of Transactions

Feature	Feature Applicability
Audit Logging	X
Authentication (Person)	X
Authentication (System)	X
Data Integrity Checking	X
Error Handling	X
HIPAA De-Identification	
Holding Messages	
Non-repudiation	X
Patient Summary	
Pseudonymize and Re-Identify	
Secure Transport	X
Transmit Disambiguated Identities	X

***Logical Registries Referenced by Transactions***

<b>Registry</b>	<b>Used</b>
Consumer	X
Patient	
Provider	
PHR Record Location	
EHR Record Location	
Consumer Permissions	
Consumer Data Sharing Preferences	
Organizational Participant	
System/Network	X

## Annex 8. Provide Data to Secondary Users

### *Description*

Source systems such as EHRs and PHRs will utilize data selection parameters to identify records of interest to secondary users. They may receive those parameters using the interchange capabilities described in Annex 6. Manage Data Selection Parameters for Secondary Use. These records will be forwarded to the NHIE. The NHIE will identify the secondary users that should receive the records and forward them directly or through other NHIEs.

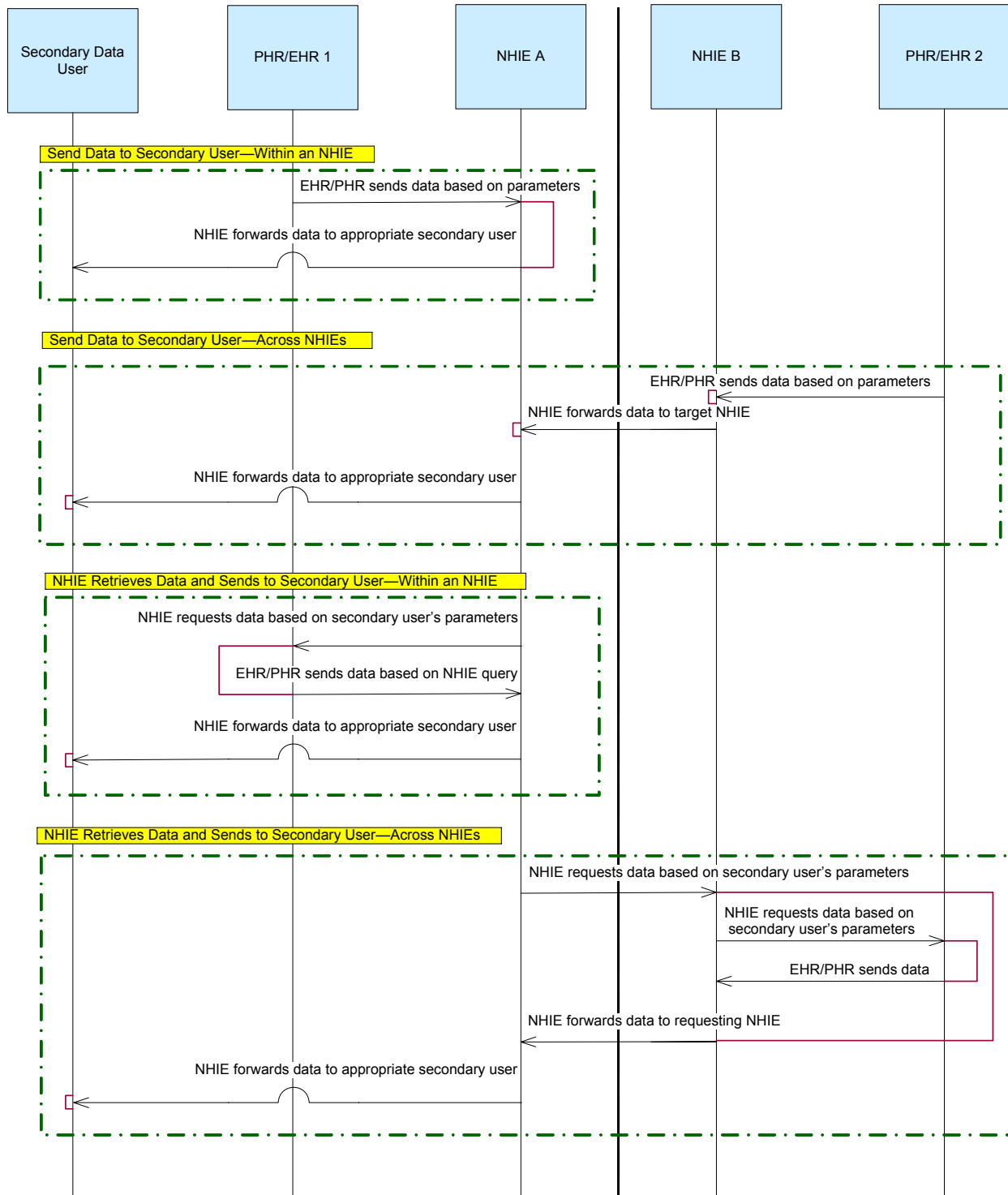
The NHIE may also support secondary user by gathering data from source systems by making queries. In this approach, the NHIE uses the secondary users' parameters to formulate a query to the source systems to request data that meets the secondary users' criteria. The source systems return the data to the NHIE, where it may be sent as individual records or held and sent in a batch.

### *Illustrative Example*

State quality-monitoring organizations collect data from hospitals to provide an annual comparison of performance on treatment of myocardial infarction. The quality-monitoring organizations provide specifications for the data to be collected, e.g., patient characteristics, diagnoses, procedures and medications. Hospital EHRs apply the specifications to their systems to select the data to send to the quality-monitoring organization. The selected data are pseudonymized and forwarded from the hospital to the NHIE. The NHIE reviews the data and forwards the data to the appropriate state quality-monitoring organization.

In a second example, a researcher has requested pseudonymized data on lab results for patients with diabetes. The NHIE sends a query to the EHRs and PHRs in its network requesting lab results for patients with a diagnosis of diabetes. The EHRs and PHRs return the requested data. In some cases the EHR or PHR is unable to pseudonymize the data before sending it to the NHIE. For those records, the NHIE pseudonymizes the data and forwards all pseudonymized records to the researcher.

**Diagram**



## **Transactions**

### **Send Data to Secondary User—Within an NHIE**

PHR/EHR 1 sends data based on parameters—PHR/EHR 1 identifies records that meet the specifications of the secondary user. These records are forwarded to NHIE A.

NHIE A forwards data to appropriate secondary data user—NHIE A reviews the data and determines the secondary data user that should receive the data. NHIE A forwards the data to the secondary data user.

### **Send Data to Secondary User—Across NHIEs**

PHR/her 2 sends data based on parameters—PHR/EHR 2 identifies records that meet the specifications of the secondary user. These records are forwarded to NHIE B.

NHIE B forwards data to NHIE A—NHIE B reviews the data and determines that the secondary user that should receive the data is associated with NHIE A. NHIE B forwards the data to NHIE A.

NHIE A forwards data to appropriate secondary user—NHIE A forwards the data to the appropriate secondary user.

### **NHIE Retrieves Data and Sends to Secondary User—Within an NHIE**

NHIE A requests data based on secondary use parameters—NHIE A sends a query to PHR/EHR 1 to obtain data that meet the selection criteria of the secondary user.

EHR/PHR 1 sends data based on NHIE A query—PHR/EHR 1 systems examine their data and identify data that meet the specifications of the secondary user. These records are forwarded to the NHIE A.

NHIE A forwards data to appropriate secondary user—NHIE A provides data to the secondary user.

### **NHIE Retrieves Data and Sends to Secondary User—Across NHIEs**

NHIE A requests data based on secondary use parameters—NHIE A sends a query to NHIE B to obtain data that meet the selection criteria of the secondary user.

NHIE B requests data based on secondary user parameters—NHIE B sends a query to PHR/EHR 2 to obtain data that meet the selection criteria of the secondary user.

PHR/EHR 2 sends data based on NHIE B query—PHR/her 2 identify data that meet the specifications of the secondary user. These records are forwarded to NHIE B.

NHIE B forwards data NHIE A—NHIE B forwards the data to NHIE A.

NHIE A forwards data to appropriate secondary user—NHIE A provides data to the secondary user.

**Common Features of Transactions**

Feature	Feature Applicability
Audit Logging	X
Authentication (Person)	X
Authentication (System)	X
Data Integrity Checking	X
Data Routing and Look-Up Proxies	X
Error Handling	X
HIPAA De-Identification	X
Holding Messages	X
Non-repudiation	X
Patient Summary	
Pseudonymize and Re-Identify	
Secure Transport	X
Transmit Disambiguated Identities	X

**Logical Registries Referenced by Transactions**

Registry	Used
Consumer	X
Patient	X
Provider	X
PHR Record Location	X
EHR Record Location	X
Consumer Permissions	X
Consumer Data Sharing Preferences	X
Organizational Participant	X
System/Network	X

## Annex 9. Pseudonymize and Re-Identify Data

### *Description*

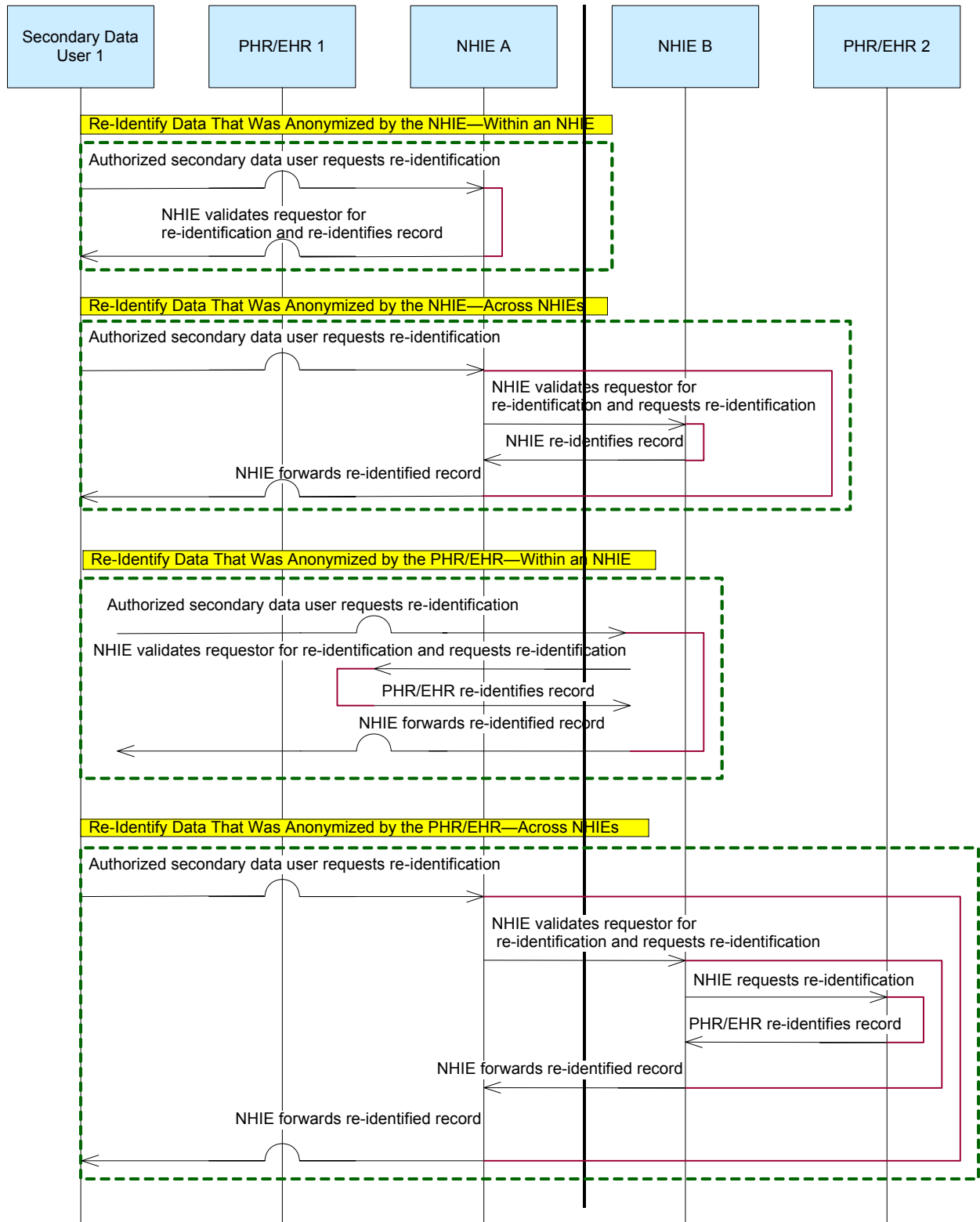
For some purposes, such as research, patient-identifying information must be removed before it is shared. In these instances, the NHIE will pseudonymize or de-identify the patient data prior to sharing the data with secondary data users. PHRs and EHRs may also pseudonymize or de-identify patient data prior to sending it to the NHIE for secondary use. There may be instances that require pseudonymized data to be re-identified, e.g., when public health officials must contact a patient regarding a communicable disease. When this occurs, the NHIE will review the request for re-identification to determine if the source of the request is authorized to receive re-identified data. If the NHIE pseudonymized the data, the data will be re-identified by the NHIE and forwarded to the authorized requestor. If a PHR or EHR pseudonymized the data, the NHIE will forward the request for re-identification to the source system. The source system will re-identify the data and return the identified records to the NHIE. The NHIE will forward the re-identified record to the authorized requestor.

Note: The description and transactions here are about re-identification. This is because pseudonymization is an option associated with several interchange capabilities. It is treated as a common feature mentioned in the corresponding annexes.

### *Illustrative Example*

The state public health agency compiles data on the incidence of specific conditions among school-age children. A community health center in a rural area of the state has an EHR system but it does not have the capability pseudonymize data. The community health center sends patient data required for public health reporting through its regional NHIE. The NHIE pseudonymizes the community health center's data and forwards the pseudonymized data to the state health agency. Officials at the state public health agency identify a record that shows the patient has tuberculosis. The state public health agency is mandated to follow up on all cases of tuberculosis to confirm that the patient has undergone treatment and to identify any individuals who have been in contact with the patient and should be screened for tuberculosis. In order to carry out this follow-up, the state public health agency sends a request to the NHIE for the record to be re-identified. The NHIE verifies that the state public health agency is authorized to receive re-identified records. The NHIE re-identifies the record and sends the identifiable record to the state public health agency.

### Diagram



## Transactions

### Re-Identify Data That Was Pseudonymized by the NHIE—Within an NHIE

Authorized secondary data user requests re-identification—A secondary user requests that NHIE A provide identifying information that was removed from patient data sent to the secondary user.

NHIE A validates requestor for re-identification and re-identifies record—NHIE A confirms that the requestor is authorized to request re-identification. NHIE A adds the identifying information to the record and forwards it to the secondary user.

### Re-Identify Data That Was Pseudonymized by the NHIE—Across NHIEs

Authorized secondary data user requests re-identification—A secondary user requests that NHIE A provide identifying information that was removed from patient data sent to the secondary user.

NHIE A validates requestor for re-identification and requests re-identification from NHIE B—NHIE A confirms that the requestor is authorized to request re-identification. NHIE A forwards the request to NHIE B that de-identified the data.

NHIE B re-identifies record—NHIE B adds the identifying information to the record and forwards it to NHIE A.

NHIE A forwards re-identified record to requestor—NHIE A forwards the re-identified data to the secondary user.

### Re-Identify Data That Was Pseudonymized by the PHR/EHR—Within an NHIE

Authorized secondary data user requests re-identification—A secondary user requests that NHIE A provide identifying information that was removed from patient data sent to the secondary user.

NHIE A validates requestor for re-identification and requests re-identification from PHR/EHR A—NHIE A confirms that the requestor is authorized to request re-identification. NHIE A forwards the request to PHR/EHR 1 that de-identified the data.

PHR/EHR 1 re-identifies data—PHR/EHR 1 adds the identifying information to the record and forwards it to NHIE A.

NHIE A forwards re-identified record to requestor—NHIE A forwards the re-identified data to the secondary user.

### Re-Identify Data That Was Pseudonymized by the PHR/EHR—Across NHIEs

Authorized secondary data user requests re-identification—A secondary user requests that NHIE A provide identifying information that was removed from patient data sent to the secondary user.

NHIE A validates requestor for re-identification and requests re-identification from NHIE B—NHIE A confirms that the requestor is authorized to request re-identification. NHIE A forwards the request to NHIE B that de-identified the data.

NHIE B requests re-identification—NHIE B forwards the request to PHR/EHR 2 that de-identified the data.

PHR/EHR 2 re-identifies record—PHR/EHR 2 adds the identifying information to the record and forwards it to NHIE B.

NHIE B forwards re-identified record to NHIE A—NHIE B sends the re-identified data to NHIE A.

NHIE A forwards re-identified record to requestor—NHIE A provides the re-identified data to the secondary user.

**Common Features of Transaction**

Feature	Feature Applicability
Audit Logging	X
Authentication (Person)	X
Authentication (System)	X
Data Integrity Checking	X
Error Handling	X
HIPAA De-Identification	
Holding Messages	
Non-repudiation	X
Patient Summary	
Pseudonymize and Re-Identify	X
Secure Transport	X
Transmit Disambiguated Identities	X

**Logical Registries Referenced by Transactions**

Registry	Used
Consumer	
Patient	
Provider	
PHR Record Location	
EHR Record Location	
Consumer Permissions	
Consumer Data Sharing Preferences	
Organizational Participant	X
System/Network	X

## **Annex 10. Publish PHR Location**

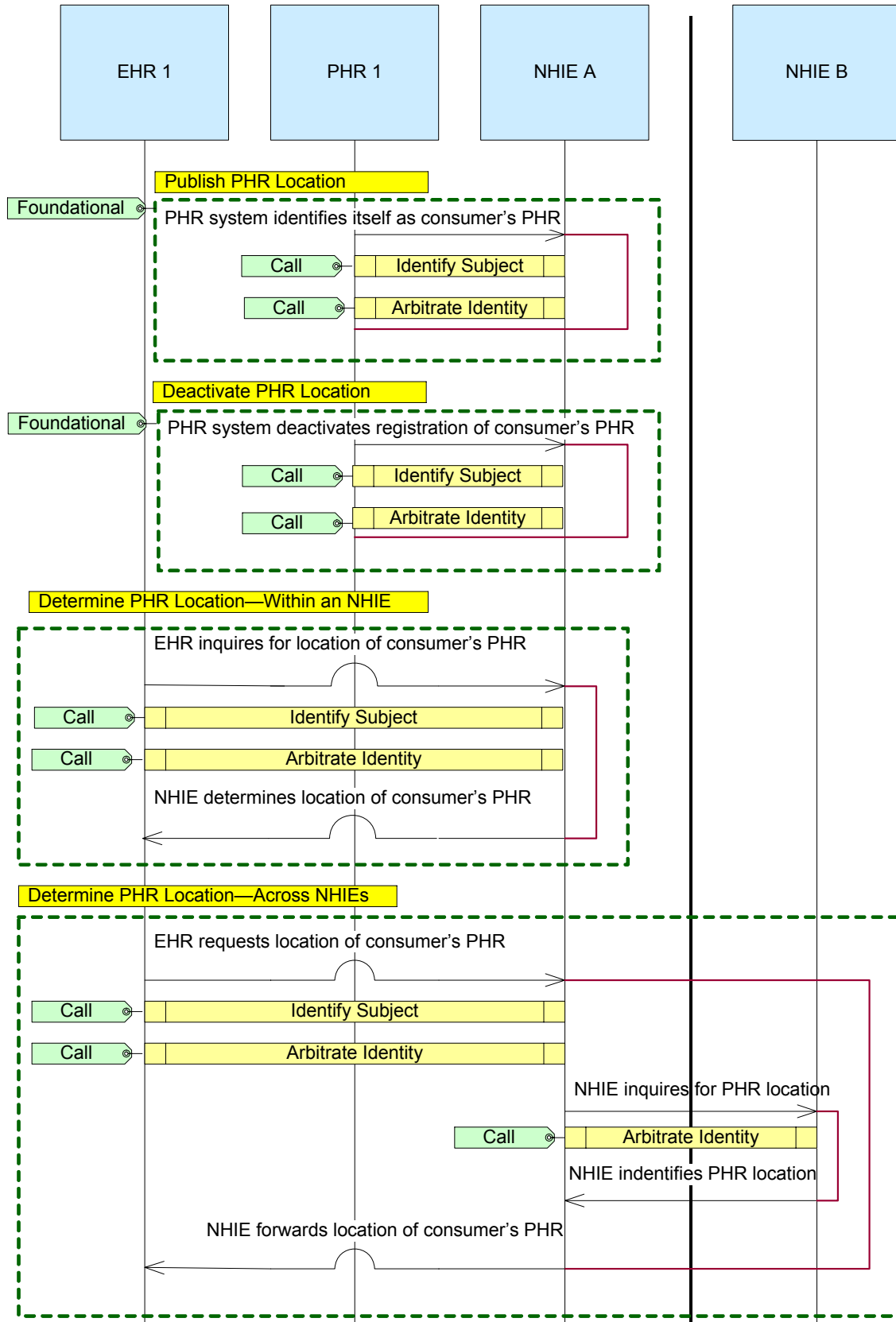
### ***Description***

As consumers create their own Personal Health Records (PHRs), there will be a need to share data from their PHRs to their providers. This data exchange requires that NHIE systems provide services that identify where the consumer's PHR data are stored and appropriately share the location with the consumer's providers. This interchange capability also enables routing based on consumer preferences as described in Annex 14. Route Data Based on Consumer-Specified Preferences.

### ***Illustrative Example***

Jane is a 52-year-old consumer who has created a Personal Health Record using a consumer portal that focuses on PHRs for patients with chronic conditions. Jane wants to use the PHR to assist her in managing her diabetes. She plans to record her daily blood sugar readings, weight and dietary intake. After establishing her PHR, Jane is asked if she would like to have her PHR registered with the NHIE so that her PHR records can be located by her providers. Jane indicates that she would like to register her PHR with the NHIE. With Jane's authorization, the PHR system notifies the NHIE that Jane has a PHR. A few weeks later, Jane has a routine appointment with Dr. Winchell. During the visit, Jane informs Dr. Winchell that she has a PHR. With Jane's permission, Dr. Winchell requests the location of the PHR. Dr. Winchell's EHR requests the data location of Jane's PHR from the NHIE. The NHIE informs Dr. Winchell's EHR system of Jane's PHR location. With this information, Dr. Winchell and Jane are able to access and download the information in Jane's PHR.

**Diagram**



## **Transactions**

### **Publish PHR Location**

PHR 1 system identifies itself as consumer's PHR—Upon enrolling in a PHR (or at any other time), the consumer's PHR address is registered with the NHIE.

### **Deactivate PHR Location**

PHR 1 system deactivates registration of consumer's PHR—Consumers may change their decision to register their PHR or move from one PHR to another. In these instances, the PHR registration would be withdrawn from NHIE A.

### **Determine PHR Location—Within an NHIE**

EHR 1 requests location of a consumer's PHR (that is within the NHIE)—A consumer's provider's EHR requests that the NHIE locate the address of the consumer's PHR.

NHIE A identifies the location of the consumer's PHR (that is within the NHIE)—After locating the consumer's PHR address, NHIE A notifies EHR 1 of the consumer's PHR location.

### **Determine PHR Location—Across NHIEs**

EHR 1 requests location of consumer's PHR (that is not within the NHIE)—A consumer's provider's EHR requests that the NHIE locate the address of the consumer's PHR.

NHIE A inquires for PHR location—NHIE A determines that the consumer's PHR is not located within NHIE A. NHIE A queries NHIE B to identify the location of the consumer's PHR.

NHIE B forwards location of consumer's PHR—NHIE B returns data on the location of the consumer's PHR.

NHIE A forwards location of consumer's PHR—After locating the consumer's PHR address, NHIE A notifies EHR 1 of the consumer's PHR location.

***Common Features of Transactions***

<b>Feature</b>	<b>Feature Applicability</b>
Audit Logging	X
Authentication (Person)	X
Authentication (System)	X
Data Integrity Checking	X
Error Handling	X
HIPAA De-Identification	
Holding Messages	
Non-repudiation	X
Patient Summary	
Pseudonymize and Re-Identify	
Secure Transport	X
Transmit Disambiguated Identities	X

***Logical Registries Referenced by Transactions***

<b>Registry</b>	<b>Used</b>
Consumer	X
Patient	
Provider	
PHR Record Location	X
EHR Record Location	
Consumer Permissions	
Consumer Data Sharing Preferences	
Organizational Participant	X
System/Network	X

## Annex 11. Retrieve Data

### *Description*

The NHIE enables consumers to access their own records, and enables providers to view or access patient records within or across NHIEs. There are several policy issues that may impact the implementation of this function, including differing policies on a consumer's right to access certain kinds of data about him or her and requirements for NHIEs to limit provider retrieval of data from other providers based on specific permissions declared by consumers. This function is modeled to support the range of these policy determinations.

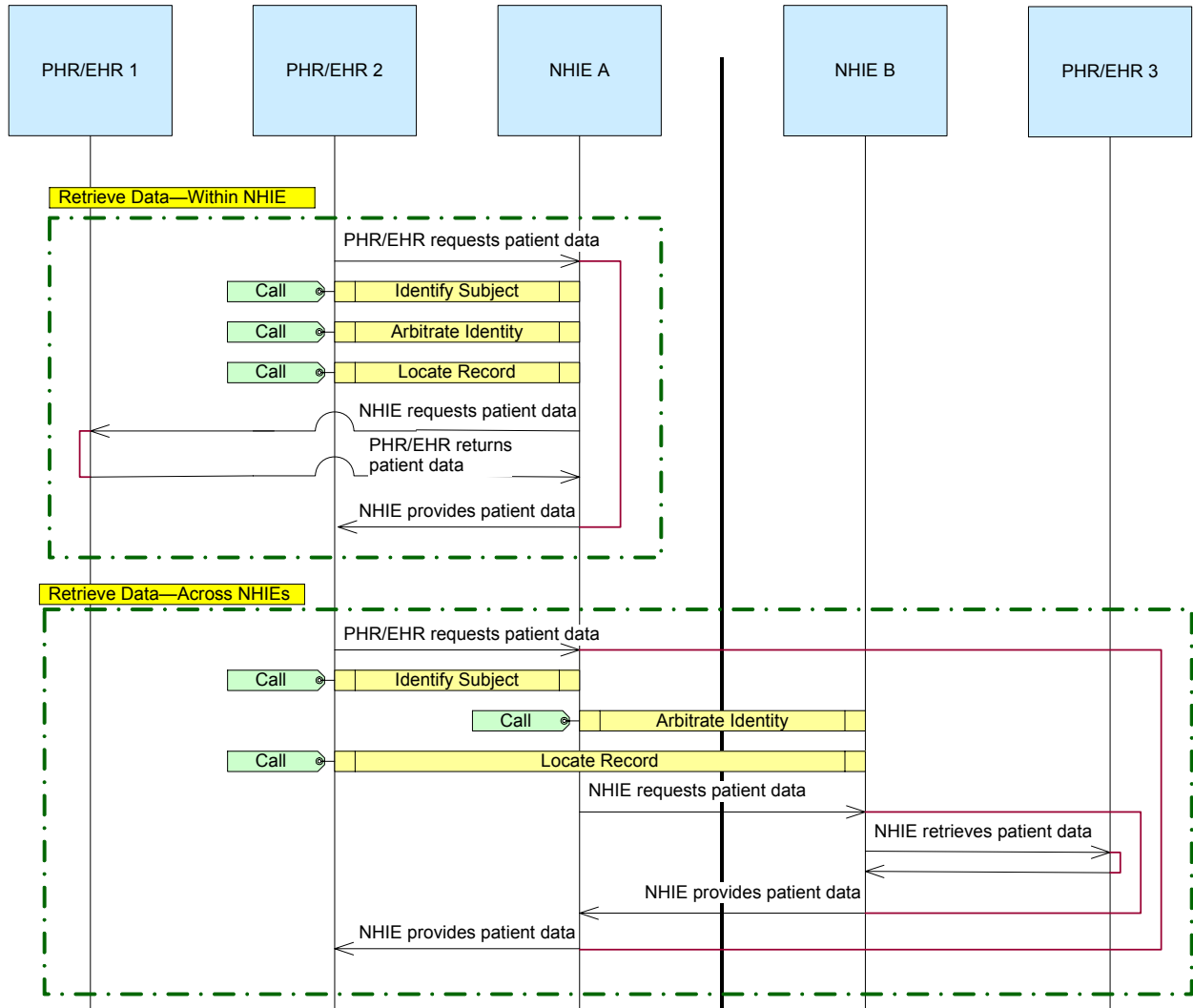
When a consumer or provider requests records, the NHIE determines the location of relevant records, determines which data to deliver based on applicable policy or consumer permissions, retrieves the data, and sends them to the requesting provider or consumer.

Data retrieval can include both individual records for a patient, e.g., lab results, and patient summary records or the individual items required to create a summary patient record.

### *Illustrative Example*

Dr. Samuels is informed by her patient, Mr. Carlson, that he had a recent visit to the cardiologist. Both Dr. Samuels' EHR system and the cardiologist's EHR system participate in the same local NHIE. Dr. Samuels requests the NHIE to retrieve these records and return them to her EHR. The NHIE requests the records from the cardiologist and forwards them to Dr. Samuels' EHR system. Mr. Carlson has also had a consultation with an endocrinologist at a research center outside of the local NHIE area. Dr. Samuels makes a request to the NHIE for these records. The NHIE requests the records from the NHIE in which the endocrinologist's office participates. The receiving NHIE retrieves the records from the endocrinologist's EHR and forwards them to the requesting NHIE. The requesting NHIE returns the records to Dr. Samuels' EHR system.

### Diagram



**Transactions****Retrieve Data—Within NHIE**

PHR/EHR 2 requests patient data—A consumer or provider requests data from a specific location.

NHIE requests patient data—NHIE A requests the data from PHR/EHR 1 and receives the requested data.

PHR/EHR 1 returns patient data— PHR/EHR 1 returns the data to NHIE.

NHIE A provides patient data—NHIE A forwards the requested data to PHR/EHR 2.

**Retrieve Data—Across NHIEs**

PHR/EHR 2 requests patient data—A consumer or provider requests data from a specific location that is outside the area of NHIE A.

NHIE A requests patient data—NHIE A requests the data from NHIE B where the organization with the record participates.

NHIE B retrieves patient data—NHIE B requests and retrieves the data from PHR/EHR B.

NHIE B provides patient data—NHIE B forwards the data to NHIE A.

NHIE A provides patient data to PHR/EHR 2—The NHIE A forwards the requested data to PHR/HER 2.

**Common Features of Transactions**

Feature	Feature Applicability
Audit Logging	X
Authentication (Person)	X
Authentication (System)	X
Data Integrity Checking	X
Error Handling	X
HIPAA De-Identification	
Holding Messages	X
Non-repudiation	X
Patient Summary	X
Pseudonymize and Re-Identify	
Secure Transport	X
Transmit Disambiguated Identities	X

**Logical Registries Referenced by Transactions**

Registry	Used
Consumer	X
Patient	X
Provider	X
PHR Record Location	X
EHR Record Location	X
Consumer Permissions	X
Consumer Data Sharing Preferences	X
Organizational Participant	X
System/Network	X

## Annex 12. Route Consumer Request to Correct Data

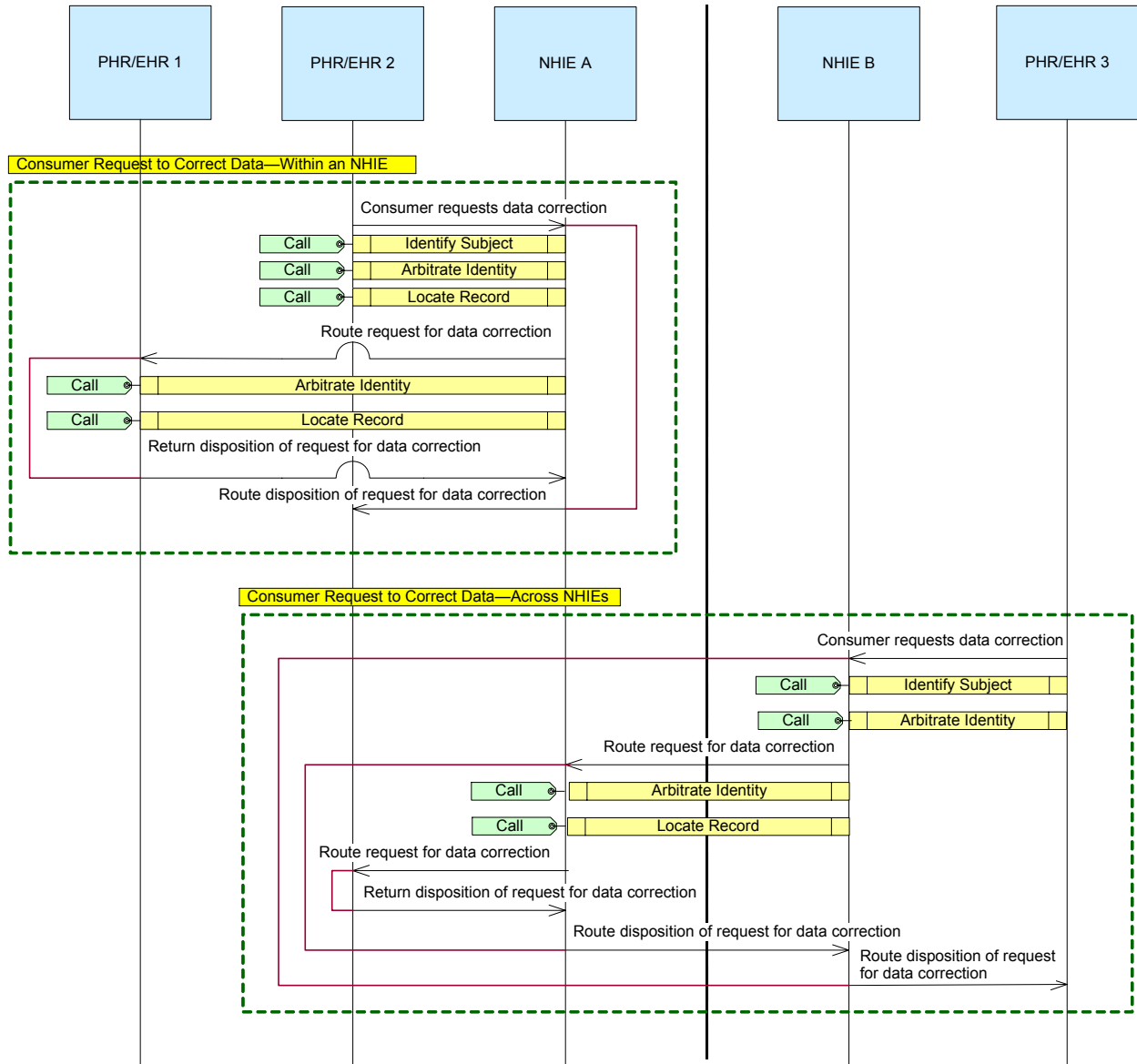
### *Description*

Consumers may identify erroneous data in their PHR that were received from other sources, e.g., a report of a test provided by a lab or specialist. The consumer can request that this be corrected at the source system. The organization operating the source system must determine if there is an error in the data, amend the data if there is an error, and notify the consumer of the action.

### *Illustrative Example*

Mr. Burton has a PHR that automatically receives reports from the various specialists he sees for his diabetes. As Mr. Burton reviews his PHR, he notices that there is a recent report from a Dr. Footwell, a podiatrist whom Mr. Burton saw recently. That report describes disabling neuropathy. Mr. Burton's blood sugar is well-controlled, and he does not have the problems described in the report. Mr. Burton submits through his PHR a request to correct this report. The PHR routes this request to the NHIE in which the PHR participates. The NHIE confirms Mr. Burton's identity and determines that Dr. Footwell is associated with another NHIE. The NHIE associated with the PHR routes Mr. Burton's correction request to the NHIE associated with Dr. Footwell. The second NHIE forwards Mr. Burton's correction request to Dr. Footwell. Dr. Footwell reviews her records and determines that the report was attached to the wrong patient. She sends out a correcting report for Mr. Burton, takes appropriate action for the other patient, and returns a notification to her NHIE that the error has been corrected. Her NHIE routes the request back through the first NHIE to Mr. Burton's PHR.

**Diagram**



## **Transactions**

### **Consumer Request to Correct Data—Within an NHIE**

Consumer requests data correction—A consumer asks for a correction to data in their PHR that was provided by another system.

NHIE A routes request for data correction to PHR/EHR 1—NHIE A routes the request for correction to PHR/EHR 1 to handle the correction request.

PHR/EHR 1 returns disposition of request for data correction—Appropriate users in the source organization review their records. If there is an error, the user takes corrective action. In any event, the user sends a notification of its action to NHIE A.

NHIE A routes response to request for data correction to the consumer—NHIE A routes the determination of the source system to the PHR/EHR 2.

### **Consumer Request to Correct Data—Across NHIEs**

Consumer requests data correction—A consumer asks for a correction to data in their PHR that was provided by another system.

NHIE B routes request for data correction NHIE A—NHIE B determines that the source system for the data is associated with NHIE A and forwards the request to NHIE A.

NHIE A routes request for data correction to PHR/EHR 2—NHIE A determines the source organization for the data and routes the request for correction to PHR/EHR 2 to handle the correction request.

PHR/EHR 2 returns disposition of request for data correction—Appropriate users in the source organization review their records. If there is an error, the user takes correction action. In any event, the user sends a notification of its action to NHIE A.

NHIE A routes disposition of request for data correction to NHIE B—The NHIE A routes the determination of the source system to NHIE B.

NHIE A routes disposition of request for data correction to consumer—The NHIE B routes the determination of the source system to PHR/EHR 3.

***Common Features of Transactions***

<b>Feature</b>	<b>Feature Applicability</b>
Audit Logging	X
Authentication (Person)	X
Authentication (System)	X
Data Integrity Checking	X
Error Handling	X
HIPAA De-Identification	
Holding Messages	
Non-repudiation	X
Patient Summary	X
Pseudonymize and Re-Identify	
Secure Transport	X
Transmit Disambiguated Identities	X

***Logical Registries Referenced by Transactions***

<b>Registry</b>	<b>Used</b>
Consumer	X
Patient	X
Provider	X
PHR Record Location	X
EHR Record Location	X
Consumer Permissions	
Consumer Data Sharing Preferences	
Organizational Participant	X
System/Network	X

## Annex 13. Route Data

### *Description*

For some messages, an NHIE may need to determine the identity of the receiving person and organization based on a name or other attributes that do not directly identify the system to receive the message. For example, there may be a need to route data to a physician whose name is identified as receiving a copy. The NHIE will have to determine from the name, and perhaps other demographic information about the physician, how to route the message to a specific system. This matching may require that the NHIE reference data about the provider, the organization that the provider is associated with, and the system in that organization that should be the target destination for the message.

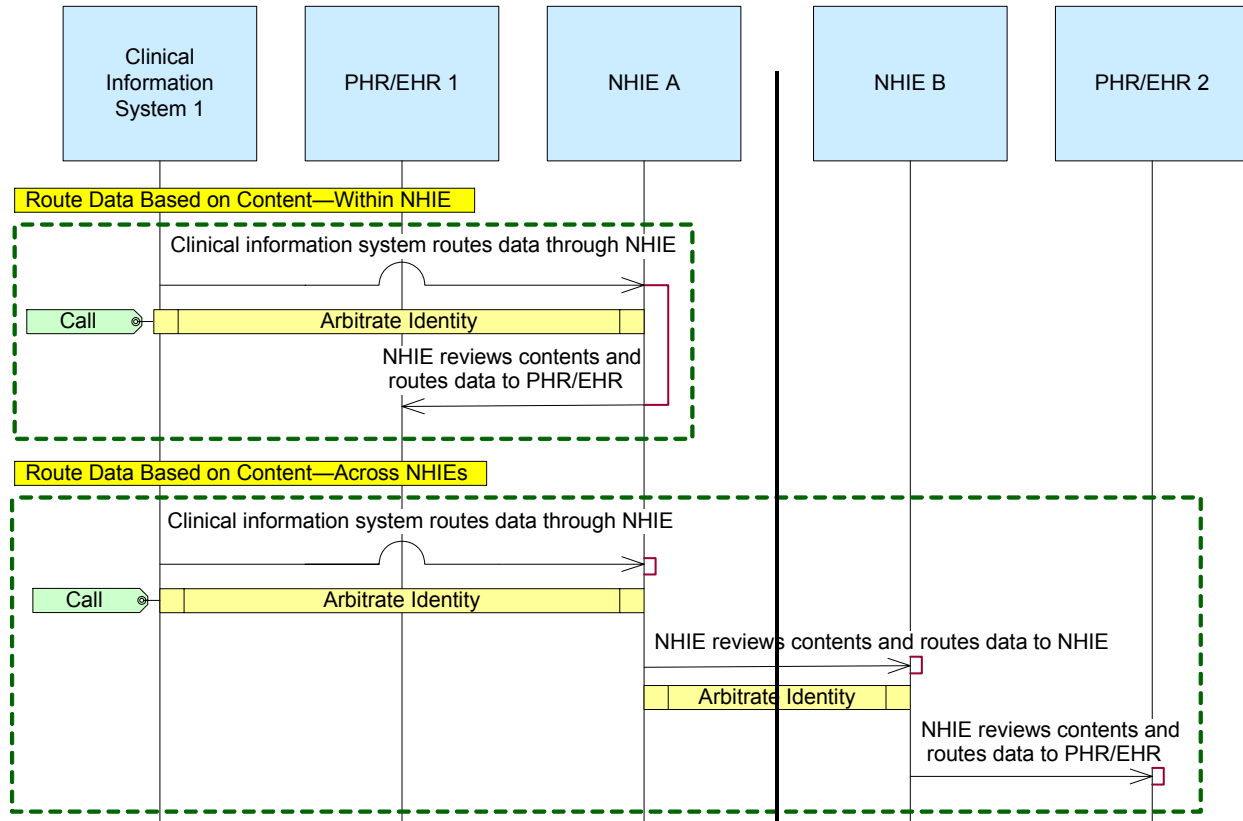
The NHIE reviews these contents to identify the subject that should receive the message and the CDO or system where the message should be sent. If policy so dictates, the NHIE may also confirm that the consumer permissions grant the recipient access to the data being routed. The NHIE uses its facilities to disambiguate provider names and consumer positions to determine recipients, and then distributes the messages. The distribution may be within the NHIE or across NHIEs. It is possible that the NHIE will not be able to unambiguously identify the recipient. NHIEs will have to handle this situation, but it is not modeled here.

The types of data routed can include both individual records for a patient, e.g., lab results, and patient summary records or the items required to create a summary patient record.

### *Illustrative Example*

Dr. Haskins has ordered a lab test for Mr. Ross. As part of the order, Dr. Haskins requests that copies of the lab test results be sent to Dr. Williams, who is consulting with Dr. Haskins on Mr. Ross' healthcare. Dr. Haskins and the laboratory participate in the same NHIE. Dr. Williams is a specialist affiliated with an Academic Medical Center that is associated with a different NHIE. Mr. Ross goes to the lab and has the test performed. The results of the lab test are sent electronically through the NHIE in which both the lab and Dr. Haskins participate. The results message indicates that both Dr. Haskins and Dr. Williams should receive copies of the test results. The NHIE reviews its provider registry and locates a record that matches Dr. Haskins. The NHIE is unable to locate a record in its subject registry for Dr. Williams. The NHIE makes a query to the NHIE associated with the Academic Medical Center where Dr. Williams practices. The second NHIE locates Dr. Williams' record and sends back to the querying NHIE information to identify Dr. Williams and the CDO where he practices. The NHIE reviews this information and confirms the match. Using this information, the NHIE forwards the lab result to the second NHIE, where it is sent to the EHR system that Dr. Williams uses.

**Diagram**



**Transactions**

**Route Data Based on Content—Within NHIE**

Clinical information system routes data through NHIE A—A clinical information system routes a message, such as a lab result, through NHIE A for delivery to recipients identified in the message.

NHIE A reviews contents and routes data to PHR/EHR 1—NHIE A reviews the contents of the message to identify the recipients and the CDOs or systems where the message should be sent. If necessary, NHIE A references its subject registry to identify the recipient and may request identifying subject information from the sending or receiving systems to confirm the recipient’s identify and ensure correct routing.

**Route Data Based on Content—Across NHIEs**

Clinical information system routes data through NHIE A—A clinical information system routes a message, such as a lab result, through NHIE A for delivery to recipients identified in the message.

NHIE A reviews contents and routes data to NHIE B—NHIE A reviews the contents of the message to identify the recipients and the CDOs or systems where the message should be sent. NHIE A determines that a designated recipient or system is associated with NHIE B. NHIE A requests that NHIE B determine if the recipient matches a subject in NHIE B’s subject registry. NHIE A confirms the subject match and forwards the message to NHIE B for routing to the recipients.

NHIE B reviews contents and routes data to PHR/EHR 2—NHIE B reviews the contents of the message and forwards it to PHR/EHR 2.

**Common Features of Transactions**

Feature	Feature Applicability
Audit Logging	X
Authentication (Person)	X
Authentication (System)	X
Data Integrity Checking	X
Data Routing and Look-Up Proxies	X
Error Handling	X
HIPAA De-Identification	
Holding Messages	
Non-repudiation	X
Patient Summary	X
Pseudonymize and Re-Identify	
Secure Transport	X
Transmit Disambiguated Identities	X

**Logical Registries Referenced by Transactions**

Registry	Used
Consumer	X
Patient	X
Provider	X
PHR Record Location	X
EHR Record Location	X
Consumer Permissions	X
Consumer Data Sharing Preferences	X
Organizational Participant	X
System/Network	X

## Annex 14. Route Data Based on Consumer-Specified Preferences

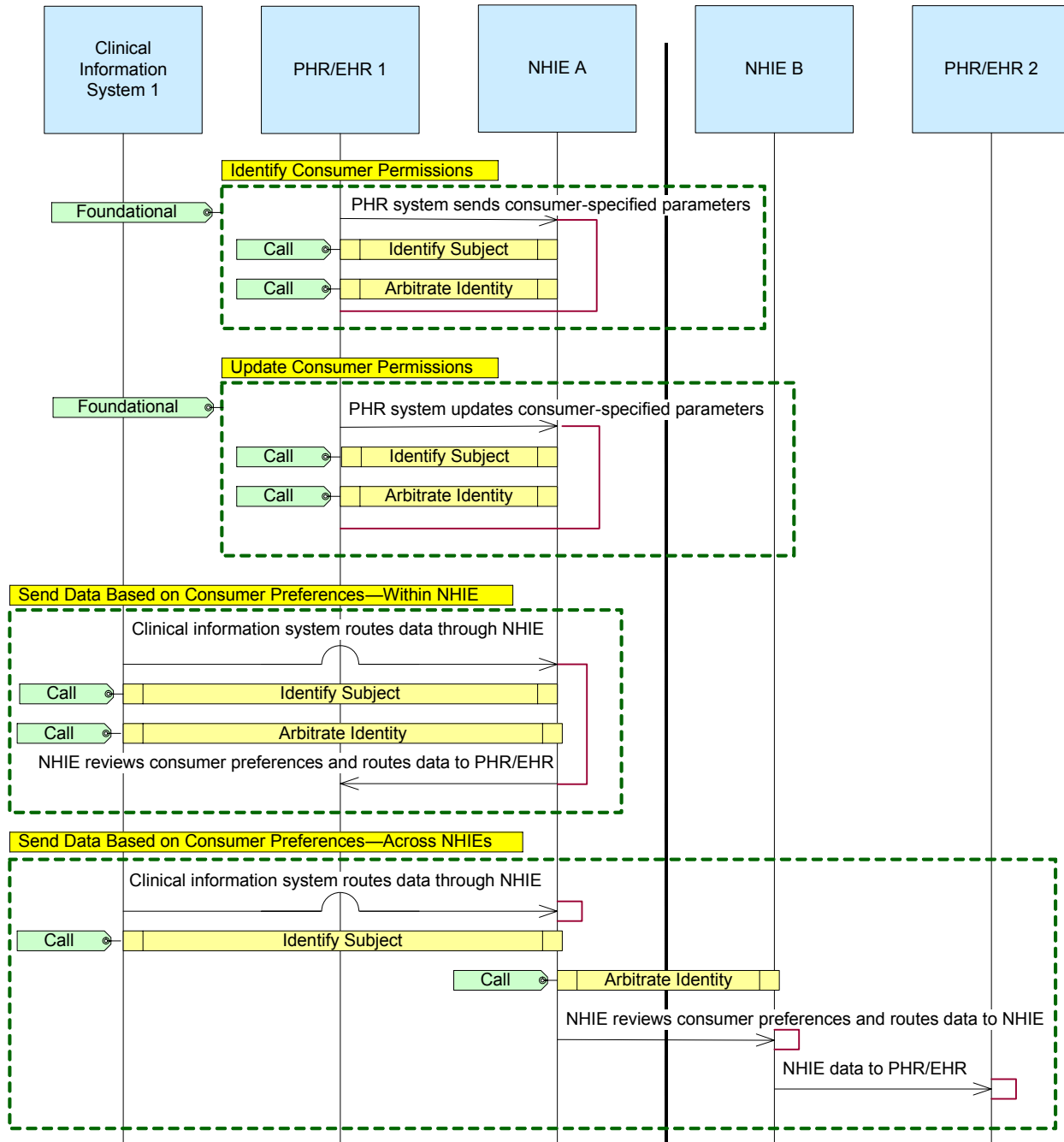
### *Description*

Consumers may determine that their PHR and specific providers should receive copies of all or selected updates to their medical information. Consumers can register and update these preferences with their NHIE. As the NHIE receives data, it compares the contents to consumer-registered preferences and forwards the data to the consumer's PHR and the consumer's specified providers. This distribution is in addition to data distribution that is based on the contents of the data received, e.g., ordering provider for a lab result.

### *Illustrative Example*

Miss Howell uses a PHR to track her medications. Miss Howell's health conditions require her to see two specialists in addition to her primary care provider. Each of these physicians has ordered medications for Miss Howell. To ensure that each provider has a complete medication profile, Miss Howell uses her PHR to indicate that each of her providers should receive copies of all her medication records. In addition, Miss Howell wants to ensure that her primary care physician has a complete picture of her health status. Using her PHR, Miss Howell indicates that her primary care physician should receive copies of results for lab tests ordered by any of her providers. As medication orders are routed through the NHIE, the NHIE determines that the order is for Miss Howell and that she has requested that a copy be sent to her all her providers. The NHIE routes copies of the medication to the providers designated by Miss Howell. A lab result for a test ordered by one of the specialists who treat Miss Howell is also routed through the NHIE. The NHIE determines that the result is for Miss Howell and that she has requested that a copy be sent to her primary care physician. The NHIE routes a copy of the result to Miss Howell's primary care physician. This copy is in addition to the NHIE routing the result to the ordering provider.

**Diagram**



## **Transactions**

### **Identify Consumer Permissions**

PHR/EHR 1 system sends consumer-specified parameters—Consumers indicate the PHR and specific providers that should receive copies of all or selected updates to their medical information.

NHIE A confirms consumer-specified parameters—NHIE A notifies the PHR/EHR 1 that the consumer-specified parameters have been added.

### **Update Consumer Permissions**

PHR/EHR 1 system updates consumer-specified parameters—Consumers update the PHR and specific providers that should receive copies of all or selected updates to their medical information.

NHIE A confirms update to consumer-specified parameters—NHIE A notifies PHR/EHR that the consumer-specified parameters have been modified.

### **Send Data Based on Consumer Preferences—Within NHIE**

Clinical information system routes data through NHIE A—Clinical information system A routes a message, such as a lab result, through NHIE A for routing and delivery.

NHIE A reviews consumer preferences and routes data to PHR/EHR 1—NHIE A reviews the contents of the message to identify the consumer/patient associated with the message. If necessary, NHIE A references its subject registry to identify the recipient and may request identifying subject information from the sending or receiving systems to confirm the recipient's identify and ensure correct routing. NHIE A reviews the consumer's preferences and routes the data to the PHR/EHR 1.

### **Send Data Based on Consumer Preferences—Across NHIEs**

Clinical information system routes data through NHIE A—A clinical information system routes a message, such as a lab result, through the NHIE A for routing and delivery.

NHIE A reviews consumer preferences and routes data to NHIE B—NHIE A reviews the contents of the message to identify the consumer/patient associated with the message. If necessary, the NHIE references its subject registry to identify the recipient and may request identifying subject information from the sending or receiving systems to confirm the recipient's identify and ensure correct routing. NHIE A reviews the consumer's preferences and routes the data to NHIE B associated with PHR/EHR 2 that the consumer identified to receive copies of his/her medical data.

NHIE B routes data to PHR/EHR 2—The NHIE B sends the data to PHR/EHR 2 as indicated by NHIE A.

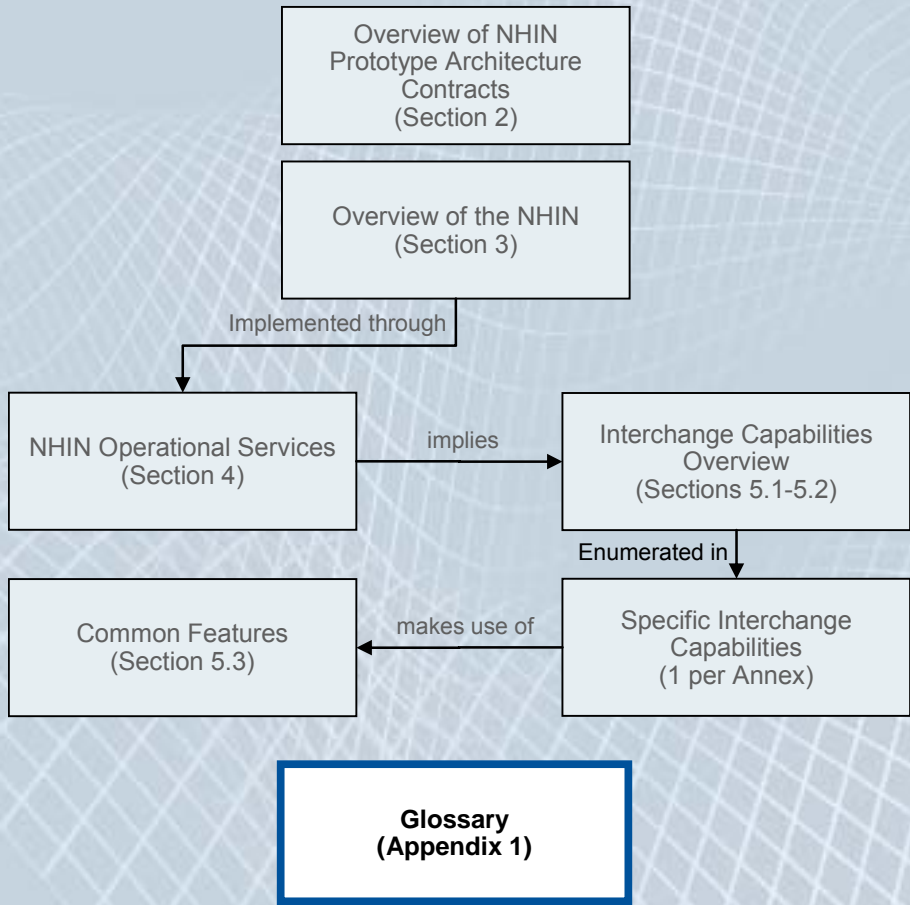
***Common Features of Transactions***

<b>Feature</b>	<b>Feature Applicability</b>
Audit Logging	X
Authentication (Person)	X
Authentication (System)	X
Data Integrity Checking	X
Error Handling	X
HIPAA De-Identification	
Holding Messages	
Non-repudiation	X
Patient Summary	X
Pseudonymize and Re-Identify	
Secure Transport	X
Transmit Disambiguated Identities	X

***Logical Registries Referenced by Transactions***

<b>Registry</b>	<b>Used</b>
Consumer	X
Patient	X
Provider	X
PHR Record Location	X
EHR Record Location	X
Consumer Permissions	
Consumer Data Sharing Preferences	X
Organizational Participant	X
System/Network	X

■ ■ ■ ■ **Glossary**



## Appendix 1: Glossary

This appendix includes terms and some acronyms used in this report. Italicized entries in the definition refer to other entries in the Glossary.

Term	Definition
<b>Action</b>	In the annexes of this report, which describe <i>Interchange Capabilities</i> , an action is the smallest transmission of information shown. It describes a flow of application information from one kind of system to another. An action that is merely an acknowledgement response devoid of application information is not shown. Actions are components of <i>Transactions</i> .
<b>Authentication</b>	Verifying the identity of a user, process or device, often as a prerequisite to allowing access to resources in an information system.
<b>Authorization</b>	Granting of rights, which includes the granting of access based on access permissions.
<b>CDO</b>	Care delivery organization.
<b>Confidentiality</b>	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
<b>Consumer</b>	A role of a person who will use the NHIN, under which the user is performing actions that make use of, or control, their own health information. Consumer functions are available to a properly authorized third party, often a parent or the child of an elderly person.
<b>De-Identification (data)</b>	Removing personal identifying information from data to an extent compatible with HIPAA privacy standards. Contrast with <i>Pseudonymization</i> .
<b>Electronic Health Record System (EHR)</b>	An electronic information system providing functions that include maintaining patients' clinical information on behalf of the organization that operates the system.
<b>Health Information Exchange (HIE)</b>	A multi-stakeholder entity that enables the movement of health-related data within state, regional or non-jurisdictional participant groups.
<b>Health Information Service Provider (HSP)</b>	A company or other organization that will support one or more NHIN Participants by providing them with operational and technical health exchange services.
<b>Interchange Capabilities</b>	Sets of <i>Transactions</i> that cluster around specific operational services.
<b>Interface</b>	A means of interaction between two devices or systems that handle data.
<b>Nationwide Health Information Network (NHIN)</b>	A "network of networks" that will securely connect consumers, providers and others who have, or use, health-related data and services while protecting the confidentiality of health information. The NHIN will not include a national data store or centralized systems at the national level. Instead, the NHIN will use shared architecture (services, standards and requirements), processes and procedures to interconnect health information exchanges and the users they support.
<b>NHIE Registry</b>	A generic container for a specific class of information that might be retained by an NHIE in the performance of its services. Their being mentioned in this report should not be taken to imply where or how this information is stored. As used in this report, the term is also unrelated to clinical information systems such as tumor registries.
<b>NHIN Collaborative</b>	The body of organizations that together constitute the NHIN.

Term	Definition
<b>NHIN Core Services</b>	The set of NHIN operational services that an HIE must provide to be qualified as an NHIE.
<b>NHIN Health Information Exchange (NHIE)</b>	An HIE that implements the NHIN architecture (services, standards and requirements), processes and procedures, and participates in the NHIN cooperative.
<b>NHIN Operational Service</b>	An act or a variety of work done for others by an HIE or NHIE. (The term “service” is used in very different ways by general readers and network architects. We are using the general sense of the word.)
<b>Permissions</b>	Declaration that a properly authorized and authenticated user may have access to specific data or functions.
<b>Personal Health Record System (PHR)</b>	An electronic information system providing functions that include maintaining a consumer’s clinical information on behalf of the consumer.
<b>Pseudonymization</b>	<p>Modifying personal health information to include disguised personal identification information such that (a) the identity of the subject is not immediately apparent; (b) the information content fits the needs of the use case; and (c) it is possible for the agent that modified the data, or its designee, to restore the identity information upon authorized request. See <i>Re-Identification</i>.</p> <p>The specific identifying information that is permissible to be retained is a matter of policy and may vary based on use case. For example, a policy determination for some use cases might support the requirement for fine-grained geographical data on otherwise disguised subjects.</p>
<b>Registry</b>	See <i>NHIE Registry</i> .
<b>Re-Identification (data)</b>	To identify the patient associated with data that have previously been pseudonymized.
<b>Transaction</b>	A logical grouping of <i>Actions</i> that must all succeed or fail as a group.
<b>Transaction Package</b>	A group of <i>Transactions</i> that are used to support a stand-alone information exchange between two or more systems.