



Strategic Implementation of the National Health Information Network (NHIN)

The information in this document is subject to change without notice.

This documentation contains proprietary information, which is protected by U.S. and international copyright. All rights are reserved. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, without the express written permission of Ingenix, Inc. Copyright © 2009 Ingenix, Inc.



NHIN Background

In the last few months it has become evident that a National Health Information Network (NHIN) has the political support necessary to become a reality and to help the health care system progress to a 21st century interconnected environment. The question is no longer *what, if or when* but *how* to deploy such a network.

The ANSI HITSP has been identifying the use case scenarios that are most urgent to automate, and has identified the standards to be used for the electronic exchange of health information. The CCHIT has been certifying systems that comply with the standards, and is now in the process of preparing interoperability certification procedures. The Department of Health and Human Services (HHS) Office of the National Coordinator (ONC) for Health Information Technology has been promoting an interoperable national health information network for the last few years and has provided the necessary funding for the pilot projects that are demonstrating the technical feasibility of an interoperable NHIN. One of the necessary steps in deploying the NHIN is to have a financial funding mechanism that will provide for the long-term operation of such a network.

SUCCESSFUL INDUSTRY NETWORKS

- Financial real-time ATM and credit card transactions across the globe
- Pharmacy real-time network for PBM and payers
- HIPAA administrative simplification leading to real-time EDI

Perhaps it is time to look at how the NHIN can be built by the health care industry without the need for long-term government and grant funding. As point of reference, over the last 30 years at least three networks have been built by the corresponding industry participants from the ground up, without the need for extensive government funding:

- The financial institutions have built a secure network that spans the globe and allows the interconnection and interoperability of their systems. Starting in the '70s with a series of cash dispensers and ATM networks that were proprietary to each bank, they migrated to regional multibank networks and finally to interconnected networks that allow cash dispensers and credit card transactions to operate almost globally. What can we learn from this experience?
- The pharmacies started in the '80s by piggybacking on the X.25 network and the credit card transactions, and built a pharmacy real-time network with several pharmacy "switches" that today connects practically all of the pharmacies in the country with the PBMs and payers in real time, with pharmacy-specific functionality that includes alerts for drug interactions, formulary validation, medication history, prescriptions, and some of the functionality desirable on the NHIN. What can we learn from this experience?
- The Administrative Simplification provisions of HIPAA adopted in 2003 a set of EDI transaction standards that are being deployed either directly between providers and payers, or through clearinghouses and data aggregators. Most of the EDI traffic is still batch-oriented, but there is an increasing movement to real-time transactions. The experience of implementing HIPAA is still evolving, and it continues to have many interoperability challenges. What can we learn from this experience?

In addition to these three existing networks we are now deploying a brand new fourth "state of the art" network for the NHIN. Rather than a single network the NHIN is taking shape as a network of networks, much like the Internet itself. How can we make sure we don't repeat the mistakes, but instead leverage the lessons learned from past experiences? How can the older technology networks be "refreshed" and migrated to the state of the art represented by the NHIN? And, just as importantly, how can we benefit from these past experiences in order to build a network that is self-sustaining

and does not need extensive long-term government funding? The answer perhaps is in the *implementation*. For the last few years the health care industry has been defining the vision, the goals and objectives, the strategy, the standards, the return on the investment, the use cases and the business scenarios. There seems to be agreement, or at least consensus, on these topics. Now it is time to take the conversation to a new level: *How do we implement the strategy and deploy the network? How do we go from the proof of concept to a large scale implementation?*

There seems to be enough interest by the different participants. Most of the standards and architecture have been defined. It seems that all we need is a critical mass that is ready to adopt the NHIN, widespread support for a common deployment plan, a clear roadmap and milestones, and a good leader, and the industry will follow. The leader needs to have enough skin in the game, enough influencing power, and an excellent understanding of the dynamics of the situation. Then the cacophony will turn into music and in the next few years we will be able to benefit from the actionable information produced by the data interchange, and the entire health care system will be transformed.

A Pragmatic NHIN Deployment Approach

This white paper tries to present a very pragmatic way to deploy the NHIN by leveraging what has been built so far as stepping-stones for implementation.

We have three disconnected legacy (financial, pharmacy, EDI) networks, and are building a fourth one for the NHIN. Even though all three legacy networks support some new technology such as TCP/IP, most of the data transfers use obsolete protocols that are expensive to maintain. Can we converge these four networks into one that uses state-of-the-art technology? Would the convergence of these networks produce enough critical mass to stimulate the adoption? Would the resulting savings help pay for the cost of a new converged network? We assert that the answer to these questions is “yes”!

One advantage of converging the four networks into one, or rather, one advantage of migrating the applications from the three legacy networks to the NHIN is that they provide a critical mass of existing applications. If instead of the NHIN supporting only clinical transactions, it also supports financial, pharmacy, and EDI transactions, the return on the investment of connecting to the NHIN is much greater. A single connection that provides all services creates a compelling proposition. In fact, the physical infrastructure is already in place through the Internet, and all we need to add is the new software to enable the NHIN functionality.

Evidently the transition to using the NHIN will not happen overnight. It could take several years, and some of the participants may not transition at all. Most likely the financial transactions will continue using the financial networks forever, and some of the batch EDI transactions will continue using clearinghouses. But the support of these other transactions over the NHIN will eventually cause a substantial migration of the activity over to the NHIN, driven by business needs and economies of scale.

First Element: Standards Adoption

What do we need to jump-start this migration? The first element in the process is adoption of the standards. We need to develop a set of use case scenarios for the transmission of financial, pharmacy, and HIPAA EDI transactions over the NHIN. These are very simple use cases, compared to the clinical use cases, but they need to be developed. Once we have the use cases developed, we will all understand the problem, the scope, and what needs to be done. Then, identifying the standards is relatively easy for this domain, given the HIPAA and banking regulations. We need standards for the data format, identifiers, routing mechanism, security, authentication, etc. Some or most of these standards already exist in the NHIN or in HIPAA.

Second Element: Gateway Availability

The second element we need for the transition is the availability of gateways. Any implementation of this nature runs into the “chicken or the egg” problem. Who would connect to the NHIN for pharmacy transactions if there were no other parties with whom to exchange transactions? Having gateways that can handle the routing of transactions from the NHIN to the legacy networks, and can convert the communication protocols, is an essential component of a migration strategy. The gateways play an important role in “impedance matching” between the two networks and will need to be in place during a transition that could take several years. Some gateways, between the NHIN and the pharmacy or EDI networks, will eventually be phased out as the pharmacy and EDI networks migrate to the NHIN. Other gateways, between the NHIN and financial networks, or between two or more of the Regional HINs, could possibly continue to exist indefinitely.

Third Element: Reference Implementations

The third element for the transition involves the reference implementations of each of the standards and protocols. One of the reasons why the Internet took off so rapidly is because most implementations of the TCP/IP stack were either based on the Berkeley TCP/IP software base, or used it as reference implementation and tested their interoperability against the Berkeley IP stack. When testing a new TCP/IP implementation, interoperability with the Berkeley TCP/IP stack was used as the test target, and any problems were corrected before deployment. This helped tremendously in the interoperability testing of the different implementations, as they did not need to test against each other. Can you imagine what would have happened if each TCP/IP user had to test his or her TCP/IP stack against each web server before connecting in production? Yet this is the current situation with the X12 HIPAA transactions because there is not a reference implementation universally adopted.

SIX ELEMENTS FOR NHIN STRATEGIC IMPLEMENTATION

1. Standards Adoption
2. Gateway Availability
3. Reference Implementations
4. Compliance Verification
5. Authentication Process
6. Public Implementation Test Center

Fourth Element: Compliance Verification

The fourth element is a method to verify or certify the compliance with the standards and the interoperability with the reference implementation. From our HIPAA experience the self-proclaimed compliance with the implementation is of little or no value, as there are too many variations of interpretation of the HIPAA requirements to ensure interoperability. The combination of a reference implementation and a certification of compliance will be a giant step toward interoperability. The CCHIT has taken a leadership role in certifying the health information systems capabilities. The next step beyond certification of the systems capabilities is the certification of the actual data compliance for interoperability against the reference implementation. This could be performed by the CCHIT defining the compliance criteria and then by independent compliance laboratories validating against the CCHIT criteria, similar to the Underwriters Laboratories (UL) certification process. During the HIPAA implementation both of these tasks were done by Claredi, now part of Ingenix, and we learned that the process is better if the entity that defines the compliance criteria is independent from the entities that verify the compliance against those criteria.

Fifth Element: Authentication Process

A fifth element concerns the authentication process. While the ONC pilot projects are using different authentication technology and methodologies, we need to

be able to trust the network at a national level. It is unlikely that the entire country will agree on a single authentication mechanism. Centralized authentication could be problematic, at least with today's technology. Given that the NHIN is evolving as a network of networks, the authentication will most likely be a federated model where each of the HINs will also include its own authentication domain. In order for these networks to provide reliable trustworthy authentication across domain boundaries, there should be some standard, generally accepted authentication policies. These policies would define who gets authenticated, the credentials and attributions of the authenticated party, and some minimum requirements for the authentication process. The authentication policies may not detail the technology implementation, but, when universally accepted, allow for the authentication to be "portable" from one domain to another. The same entities that provide "private" authentication today (Medicare, payers, hospitals, IPAs, professional societies, etc.) could be the entities that provide the portable authentication in the future, by just adapting their authentication process to the standard policies.

Sixth Element: Public Implementation Test Center

Finally, the sixth element that glues all of these together would be a publicly available test center where the implementers can test their implementation. Sort of a technical workbench with all the tools necessary to test the systems. A site where the standards and the reference implementation can be downloaded, where the communications protocols can be exercised, where the data exchange messages can be tested, where the systems capabilities can be verified, where the authentication can be challenged, and where expert help can be obtained to help with problems. This sort of "technical assistance" center would go a long way toward the independent development of multiple interoperable implementations. During the initial HIPAA implementation this role was performed by Claredi, and we learned of the importance and effectiveness of it for interoperability, in spite of the many "flavors" of the HIPAA Companion Guides.

Leveraging the Work to Achieve the NHIN

The elements described here should be deployed at the national level with a sense of urgency. Some of them will need a local or regional flavor in order to support regional differences. They do not cover all the ground necessary for the NHIN, but leverage the work already in progress and leave plenty of room for implementation variations. They will serve as stepping-stones in the path toward a national interoperable *implementation* of the Health Information Network.



For Information: 800.765.6034 | ingenuity@ingenix.com
Ingenix, Inc. | 12125 Technology Dr. | Eden Prairie, MN 55344
www.ingenix.com

About the Author

Kepa Zubeldia, M.D.

Senior Vice President, Interoperability Technologies Ingenix

Dr. Kepa Zubeldia is senior vice president of interoperability technologies for Ingenix. In this role, he creates strategies for the industry's next generation of health care information exchange. Dr. Zubeldia joined Ingenix in May 2006 through the acquisition of his company, Claredi. As founder and president of Claredi, he established the nation's first commercial provider of HIPAA EDI compliance testing and certification services and led the development of pioneering health care transaction management, connectivity and information exchange technologies.

Dr. Zubeldia has been involved with health care information exchange technologies for more than 20 years and has participated in a number of industry bodies, including serving as co-chair of the Security Policy Advisory Group of the Workgroup for Electronic Data Interchange (WEDI) and chair of the Association for Electronic Health Care Transactions (AFEHCT). From 1999 to 2004, he served on the National Committee on Vital and Health Statistics (NCVHS). In 2002, Dr. Zubeldia received the Ed Guilbert E-Commerce Professional Award and the Leadership in Technology WEDI Award.

About the Company

Ingenix, a wholly-owned subsidiary of UnitedHealth Group (NYSE: UNH), transforms organizations and improves health care through information and technology. Organizations rely on its innovative products, services and consulting to improve the delivery and operations of their business. More information about Ingenix is available at www.ingenix.com.

Ingenix | Intelligence for Health Care | www.ingenix.com

From North America, call: 1-800-765-6034 • ingenuity@ingenix.com
For a list of Ingenix global office locations, please refer to our website www.ingenix.com

Corporate Headquarters | 12125 Technology Drive, Eden Prairie, MN 55344

Ingenix and the Ingenix logo are registered trademarks of Ingenix. All other brand or product names are trademarks or registered marks of their respective owners. Because we are continuously improving our products and services, Ingenix reserves the right to change specifications without prior notice. Ingenix is an equal opportunity employer.

100-1842 02/09 Original © 2009 Ingenix. All Rights Reserved.