

Towards the National Health Information Network in the United States of America

Andrew Targowski

Western Michigan University, Kalamazoo, MI 49008, USA

(269) 375-6860, andrew.targowski@wmich.edu

Abstract: The Health Infrastructure in the U.S. is called the National Health Information Network (NHIN) which is composed of regional Health Information Exchange (HIE) hubs. This approach has been exercised since 2008. However, there is a lack of one top-down comprehensive architecture of this system, which is being developing by each state individually. This paper provides the top-down model of such architecture, perhaps the first one which is made. The paper defines basic components of that system. Also some issues of security and privacy of stored and exchanged data are disputed. In the end, the paper provides conclusions regarding the issues of its implementation.

INTRODUCTION

This investigation contains the background of the current policy of the U.S. National Health Program (2011), it particularly identifies the components of that program, which later will be integrated into an architecture of health information infrastructure. Its security and privacy issues will be discussed. The conclusion will assess the feasibility of the presented architecture.

The Health Infrastructure in the U.S. is called the National Health Information Network (NHIN) which is composed of regional Health Information Exchange (HIE) hubs. This approach has been exercised since 2008. HIE is defined as the mobilization of health care information across organizations within a region, community, or hospital system. The goal of HIE is to facilitate access to and retrieval of clinical data to provide safer, more timely, efficient, effective, equitable, patient-centered care. HIE should be also useful to Public Health authorities to assist in analyses of the health of the population (Woolhandler and Himmelstein 1997).

HIE systems should facilitate physicians and clinicians in meeting high standards of patient care through electronic participation in a patient's continuity of care with multiple providers. Secondary health care providers should benefit through reduced expenses associated with duplicate tests, time involved in recovering missing patient information, paper, ink, associated office machinery, manual printing, scanning and faxing of documents, the physical mailing of entire patient charts, manual phone communication to verify delivery of traditional communications, referrals, and tests results. According to an internal study at Sushoo (FL) HIE, a single-clinician practice spends \$17,160/year associated with the current method of exchanging patient's health information (retrieved on 2010-5-31 <http://www.sushoo.com/sushoo-demo.html>).

SECURITY ISSUES OF THE NATIONAL HEALTH INFORMATION NETWORK

Recent revelations of "secure" data breaches at centralized data repositories, in banking and other financial institutions, in the retail industry, and from government databases, have caused concern about storing electronic medical records in a central location. Records that are exchanged over the Internet are subject to the same security concerns as any other type of data transaction over the Internet.

The Health Insurance Portability and Accountability Act (HIPAA) was passed in the US in 1996 to establish rules for access, authentications, storage and auditing, and transmittal of electronic medical records. This standard made restrictions for electronic records more stringent than those for paper records. However, there are concerns as to the adequacy of implementation of these standards in practice.

PRIVACY ISSUES OF THE NATIONAL HEALTH INFORMATION NETWORK

One major issue that has risen on the privacy of the U.S. network for electronic health records is the strategy to secure the privacy of patients. Former US president Bush called for the creation of networks, but federal investigators report that there is no clear strategy to protect the privacy of patients as the promotions of the electronic medical records expands throughout the United States. In 2007, the Government Accountability Office reports that there is a “jumble of studies and vague policy statements but no overall strategy to ensure that privacy protections would be built into computer networks linking insurers, doctors, hospitals and other health care providers” (Pear 2001).

The privacy threat posed by the interoperability of a national network is a key concern. One of the most vocal critics of EMRs, New York University Professor Jacob M. Appel, has claimed that the number of people who will need to have access to such a truly interoperable national system, which he estimates to be 12 million, will inevitably lead to breaches of privacy on a massive scale. Appel has written that while “hospitals keep careful tabs on who accesses the charts of VIP patients,” they are powerless to act against “a meddling pharmacist in Alaska” who “looks up the urine toxicology on his daughter’s fiancé in Florida, to check if the fellow has a cocaine habit” (Francis 2006). This is a significant barrier for the adoption of an EHR. Accountability among all the parties that are involved in the processing of electronic transactions including the patient, physician office staff, and insurance companies, is the key to successful advancement of the EHR in the U.S. Supporters of EHRs have argued that there needs to be a fundamental shift in “attitudes, awareness, habits, and capabilities in the areas of privacy and security” of individual’s health records if adoption of an EHR is to occur (Nulan 2001).

So far, The U.S. Department of Health and Human Services takes no action on complaints under HIPAA, and medical records are disclosed under court orders in legal actions such as claims arising from automobile accidents. HIPAA has special restrictions on psychotherapy records, but psychotherapy records can also be disclosed without the client’s knowledge or permission. For example, Patricia Galvin, a lawyer in San Francisco, saw a psychologist at Stanford Hospital & Clinics after her fiancé committed suicide. Her therapist had assured her that her records would be confidential. But after she applied for disability benefits, Stanford gave the insurer her therapy notes, and the insurer denied her benefits based on what Galvin claims was a misinterpretation of the notes. Stanford had merged her notes with her general medical record, and the general medical record wasn’t covered by HIPAA restrictions (Nulan 2001).

BASIC DATA ENTRY OF THE NATIONAL HEALTH INFORMATION NETWORK

The whole HIE architecture is based on a set of related electronic data entry (records), for

- Electronic Medical Records about patients (EMR)
- Electronic Laboratory Records (ELR)
- Electronic Image Records (EIR)
- Computer Physician Order Entry (CPOE) at hospitals
- Electronic Pharmacy Records (EPR)
- Personal Health Records (PHR) collected by individuals and eventually shared with appropriate health care providers
- Disease Management System (DMS), maintained by Insurers
- Other

The advantage of these electronic records is that they can “talk to each other” and reduce chaos and errors. In the United States, Great Britain, and Germany, the concept of a national centralized server model of healthcare data has been poorly received. Issues of privacy and security in such a model have been of concern.

(Retrieved on 2010-5-31; e-Health Insider (UK). January 2008. http://www.e-health-insider.com/news/3384/german_doctors_say_no_to_centrally_stored_patient_records).

Privacy concerns in healthcare apply to both paper and electronic records. According to the average medical practice, roughly 150 people (from doctors and nurses to technicians and billing clerks) have access to at least part of a patient’s records during a hospitalization, and several, providers and other entities that handle providers’ billing data have some access also (e-Los Angeles Times).

ARCHITECTURE MODEL OF THE NATIONAL HEALTH INFORMATION NETWORK

Within the private sector, many companies are moving forward in the development, establishment, and implementation of medical record banks and health information exchange.

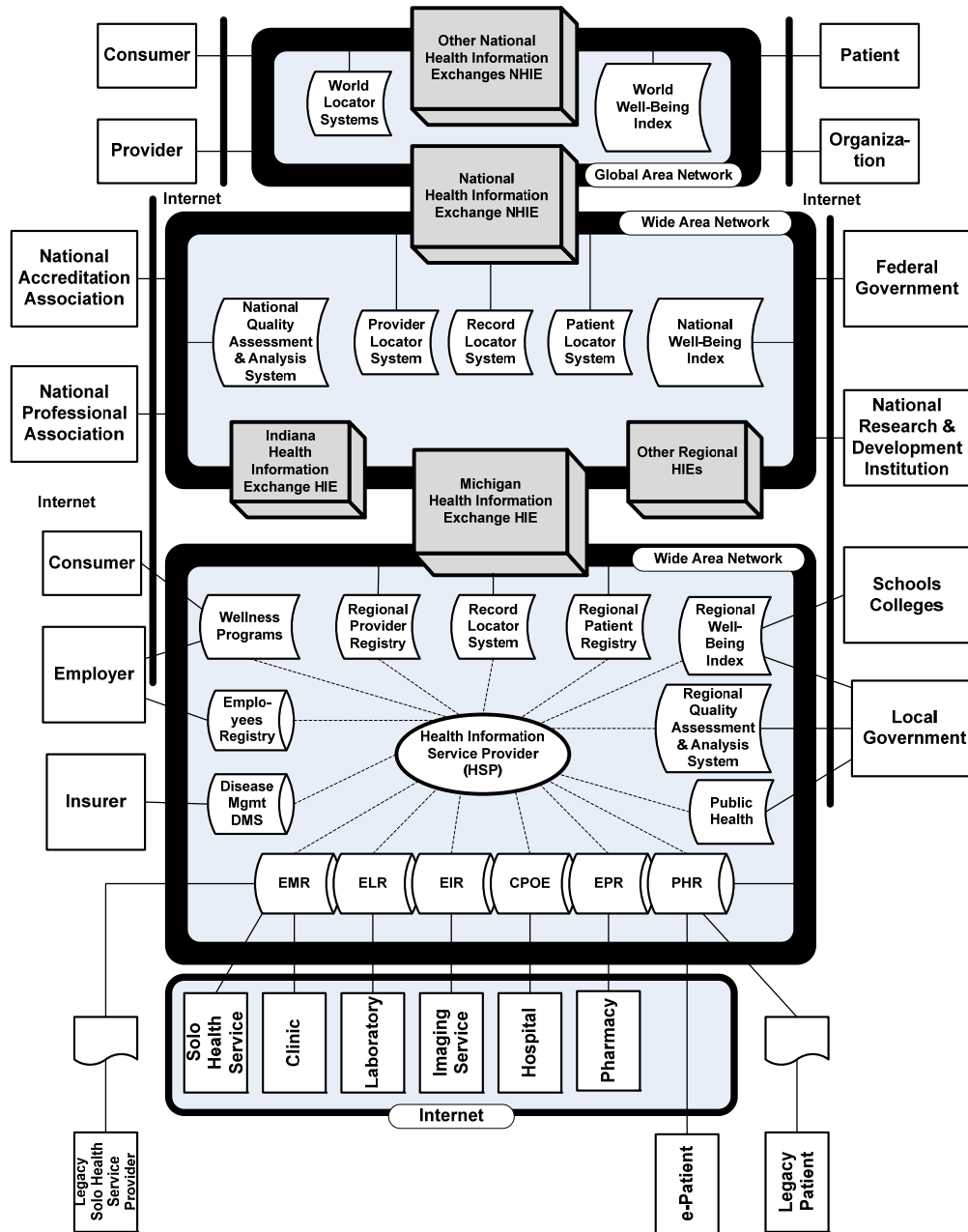


Figure 1. The Architecture of National Health Information Exchange Network for the U.S (2010) (EMR-Electronic Medical Record, ELR-Electronic Laboratory Record, Electronic Image Record, CPOE-Computerized Physician Order Entry, Electronic Pharmacy Record, Personal Health Record (The Targowski Model))

By law, companies are required to follow all HIPAA standards and adopt the same information-handling practices that have been in effect for the federal government for years. This includes two ideas: standardized formatting of data electronically exchanged and federalization of security and privacy practices among the private sector. Private companies have promised to have “stringent privacy policies and procedures.” If protection and security are not part of the systems developed, people will not trust the technology nor will they

participate in it. So, the private sector knows the importance of privacy and the security of the systems and continues to advance well ahead of the federal government with electronic health records.

In health care files and databases, paper-based systems are difficult to keep updated and to share with other health care providers and users. If a given health care provider does not have good enough information technology at hand, it can acquire services of independent Health Information Services Providers (HISP).

The architecture of Health Information Exchange Network is depicted in Figure 1. This architecture (according to this author) is based on *private* Wide Area Networks (WAN) and Global Area Network (GAN) and the Internet. The U.S. Office of National Coordinator for Health Information Technology (ONC) plans the use of the Internet only. It is recommended contrary to American businesses' practice which organized data transmission on private networks (MAN, WAN, GAN, VAN) due to higher security than which can be achieved on the Internet. According to the ONC, the NHIE will apply software which will comply with the access and security standards defined in the CONNECT Project.

The presented architecture of the HIE Network includes two very important systems at the regional and national levels: the Quality Assessment and Analysis System (QAAS) and Well-Being System (WBS). Furthermore, there planned at the regional and national levels; locators of records, patients, and providers.

SYSTEMS OF THE NATIONAL HEALTH INFORMATION NETWORK

The planned National Health Information Network has the following four levels of information processing systems:

- Level 1 "Local" – Includes health service providers, such as: health clinics, health laboratories, imaging services, hospitals and so forth. At this level health service data about patients (consumers, employers, insurers) are entered under systems' form of
 - Electronic Medical Records (EMR),
 - Electronic Laboratory Records (ELR),
 - Electronic Pharmacy Records (EPR),
 - Personal Health Records (PHR), and other.
- Level 2 – "Regional" – Includes health insuring employers, insurers, local governments, and so forth, which create the State Health Information Exchange (HIE) services, which will use the following systems;
 - Operational systems: Employees Registry, Regional Patient Registry, Regional Provider Registry, and Record Locator System,
 - Quality control systems: Regional Well-Being Index, Regional Quality Assessment & Analysis System, Public Health System,
 - Program Informing Systems: Disease Management System, Wellness Program, and so forth.
- Level 3 "National" – Includes federal government, national research & development institutions, national accreditation associations, national health professional associations which create the National Health Information Exchange (NHIE) and will use the following systems:
 - Operational systems: Provider Locator System, Patient Locator System, Records Locator System,
 - Quality control systems: National Well-Being Index, National Quality Assessment & Analysis System
 - Gateways to other regional HIE(s)
- Level 4 "International" – includes foreign health services providers, insurers, which provide services for the American patients or the American health services providers which provide services for foreign patients being treated in the U.S. They will apply the following systems:
 - Operational systems: World Locator System
 - Quality control system: World Well-Being Index.
 - Gateways to National HIE (s).

These systems create a complex system environment, which should be planned, design, and implemented with the mix strategy, including top-down provided standards and bottom-up data entry processes, controlled by the local, national, and international users. This kind of the system complex is difficult to implement, since the health care industry, the largest business in the world, is full of contradictory goals and strategies. Very often the planned "chaos" serves better than the organized systems?

CONCLUSION AND THE FUTURE WORK

At the time of publishing this paper (August 2011), the author is rather pessimistic about possibility of successful implementation of this architecture. The American national political and societal climate is negative for large-scale and innovative initiatives (Lee and Mongan 2009). The status quo is the most popular policy among established political and professional leaders (Woolhandler and Himmelstein 1997). This is because the 19th century attitude was supposedly very successful in developing of Americanism (efficient way to wealth and “happiness”).

Unfortunately, after the passing of almost two centuries, today we enter a new epoch of new societal issues and required solutions, which require bold conceptualization and tough choices, through the 21st century (Porter and Teisberg 2006). However, despites of these new challenges the most powerful country in the world must search for new ways to wealth and happiness of its citizens (Targowski 2009).

REFERENCES

- Appel, J.M. (2008). Why Shared Medical Database Is Wrong Prescription. *Orlando Sentinel*, December 30, 2008.
- Christensen, C.M. (2009). *The Innovator's Prescription. A Disruptive Solution for Health Care*. New York: McGraw Hill.
- Francis, Th. (2006). Spread of Records Stirs Fears of Privacy Erosion, *The Wall Street Journal*, December 28.
- Lee, Th. H. and J.J. Mongan. (2009). *Chaos and Organization in Health Care*. Cambridge, MA: The MIT Press.
- McGlenn et al. (2003). The Quality of Health Care Delivered to Adults in the United States. *New England Journal of Medicine*, 348(26): 2635-2645.
- Nulan, C. (2001). HIPAA--A Real World Perspective. *Radiol Manage*, 23(2): 29-37.
- Pear, R. (2001). Warnings over Privacy of U.S. Health Network. *New York Times*, February 18.
- Porter, M.E. and E.O. Teisberg. (2006). *Redefining Health Care*. Cambridge, MA: Harvard Business School Press.
- Targowski, A. (2009). *Information Technology and Societal Development*. Hershey & New York: Information Science Reference.
- Woolhandler, S. and D.U. Himmelstein. (1997). The Deteriorating Administrative Efficiency of the U.S. Health Care System. *New England Journal of Medicine*. 324(18): 1253-1258.