Managing Electronic Patient Health Information in a Nationwide Health Information Network

John C. Branner III

East Carolina University

Information Security Management

ICTN 6823

Dr. Phil Lunsford

July 17, 2018

Managing Electronic Patient Health Information in a Nationwide Health Information Network

A lack of access to medical records can cause delays and put patient health at risk. Since 2004, the U.S. government has been working toward developing a nationwide health information network (NHIN or NwHIN) to bridge the health care information gap between geographic locations and create a “network within networks.” However, problems associated with the development of the NHIN have been noted early in the development process. Patient information security, accessibility, interoperability, and data standardization have been at the forefront of concern. This paper addresses those concerns and provides a framework for managing a nationwide patient information network.

Development of the NHIN

Since 2001, U.S. government agencies have been working toward a standardized system of electronic exchange of clinical health information. The Department of Health and Human Services (HHS), the Department of Defense (DOD), the Office of Management and Budget (OMB), the Department of Veteran Affairs (VA), and several other agencies collaborated for the Consolidated Health Informatics (CHI) initiative. By 2003, the first five standards were established. By 2004, these agencies and other “Federal partners” adopted the first five and the next 15 healthcare messaging and vocabulary standards recommended under CHI (Health and Human Services Department [HHS], 2005).

During his 2004 State of the Union address, president George W. Bush called for a nationwide EHR with a 10-year target for completion (Speedie & Davies, 2006). Under order of EO13335, the Secretary of the U.S. Department of Health and Human Services established the Office of National Coordinator of Health Information Technology (ONCHIT or ONC).

EO13335

The development of the NHIN began in 2004, when president George Bush signed Executive Order 13335. The intent was to create a nationally recognized electronic health record (EHR). The main focus was placed on an interoperable, integrated, accessible EHR system that allows medical information to follow patients and to provide health care professionals with the information they need to make informed clinical decisions (Monegain, 2004). EO 13335 addressed six specific goals:

> (a) Ensures that appropriate information to guide medical decisions is available at the time and place of care;
>
> (b) Improves health care quality, reduces medical errors, and advances the delivery of appropriate, evidence-based medical care;
>
> (c) Reduces health care costs resulting from inefficiency, medical errors, inappropriate care, and incomplete information;
>
> (d) Promotes a more effective marketplace, greater competition, and increased choice through the wider availability of accurate information on health care costs, quality, and outcomes;
>
> (e) Improves the coordination of care and information among hospitals, laboratories, physician offices, and other ambulatory care providers through an effective infrastructure for the secure and authorized exchange of health care information; and
>
> (f) Ensures that patients' individually identifiable health information is secure and protected. (Exec. Order No. 13335, 2004, p. 24059)

In April 2004, Dr. David Brailer was appointed to the National Coordinator position. He was given the task of creating a strategic plan for the development, maintenance, and oversite of a nationwide health information network in both the private and public health care sectors (Brailer, 2004). Brailer's plan included four main goals to meet the task: 1) introduction of information tools into clinical practice, 2) electronically connecting clinicians to other clinicians, 3) using information tools to personalize care deliver, and 4) advancing surveillance and reporting for population health improvement (Brailer, 2004). The total framework outlined 12 strategies to meet these four goals.

Other significant parts of Dr. Brailer's plan included the development of a private sector EHR certification process and funding for community health information exchange systems. These objectives would later result in meaningful use standards and the formation of regional health information organizations (RHIOs), also known as Health Information Exchanges (HIEs). HIEs are at the core of the NHIN.

HITECH

Title XIII of the American Reinvestment and Recovery Act of 2009 addresses Health Information Technology and implements the Health Information Technology for Economic and Clinical Health (HITECH) Act. HITECH provides the first set of standards for health care information systems. These standards were designated as "meaningful use" (standards).

Meaningful use (MU) has been most notably led by the Centers for Medicare and Medicaid Services (CMS) in collaboration with the ONC (Centers for Disease Control and Prevention [CDC], 2017). The original plan to implement MU was broken up into three stages: Meaningful Use Stage 1, 2, and 3. Each Stage has a set of goals to be accomplished. However, problems with the scope and scale of implementation have caused delays and concerns over the success of MU.

Meaningful Use Stage 1

Meaningful Use Stage 1 was arguably the most successful phase of the meaningful use initiative. Starting in September 2010, CMS mandated the reporting of selected criteria for eligible providers. These included 15 core set objectives and a pick list of 10 additional criteria, in which eligible providers would select 5 of the 10 additional criteria (CDC, 2017).

MU criteria reporting raised questions for not only how to capture such information, but also how to store and report gathered data. There was even more pressure for EPs to participate because CMS offered financial incentives to those entities that were compliant. EPs not in compliance would eventually face penalties. 2014 became the last year for receiving incentives. Additionally, MU data gathered in 2014 would be the basis for 2016 Medicare payment adjustments (CDC, 2017). The timeline for MU Stage 1 was between 2011 and 2015.

Meaningful Use Stage 2

The requirements and guidelines for MU Stage 2 were released in 2012. This included a higher standard core set of reportable measures from 15 to 17 and 3 of 6 pick list items. It was also during this stage that standards for a certified EHR were set. However, the Final Rule for MU Stage 2 delayed mandatory implementation until 2014. The timeline for MU Stage 1 was between 2012 and 2016 (CDC, 2017).

Modified Meaningful Use Stage 2 (2015-2017) and Stage 3 Meaningful Use

As EHR vendors began developing “certified” systems, reporting processes became automated. This reduced the need for manual reporting systems. As a result, the required reportable criteria were modified to include measures outside the automated capabilities of certified systems. Reportable measures differ between provider types. Nonetheless, EPs entering

MU Stage 3 must report two out of five clinical measures. The timeline for MU Stage 3 is from 2017 and beyond (CDC, 2017).

Transition from NHIN to eHealth Exchange

By 2012, the ONC solicited management of the NHIN (renamed eHealth Exchange) to public vendors. The winning bidder was The Sequoia Project, a 501(c)(3) nonprofit organization. Since The Sequoia Project took over management of the eHealth Exchange, the network has grown to become the largest health information exchange network in the country. However, the project is still in its infancy and faces the same information security concerns it had since NHIN development. As described by The Sequoia Project,

> The eHealth Exchange is a group of federal agencies and non-federal organizations that came together under a common mission and purpose to improve patient care, streamline disability benefit claims, and improve public health reporting through secure, trusted, and interoperable health information exchange. (The Sequoia Project, 2018, p. 1)

This was the first step toward partnering with the public sector to make the eHealth Exchange a fully interoperable network.

Although The Sequoia Project has worked toward developing the largest national health information exchange, there is still more work to be done. Every U.S. state and territory now has a Health Information Exchange (HIE) (The Office of the National Coordinator of Health Information Technology [ONC], n.d.). However, some of the previous concerns with meaningful use, privacy, security, and interoperability remain a top priority for key stakeholders.

Managing Electronic Health Care Information

Privacy

The most basic element of the eHealth Exchange is electronic patient health information. Although having a network capable of giving patients and providers access to patient health information can improve patient care, it gives more people more access to private information. This access includes government agencies, such as the DOD, CDC, VA, the Social Security Administration, and others.

The primary participants in the eHealth Exchange are the patients (or consumers), health care providers, and the HIEs. One of the first quantitative studies (2008) for consumer attitudes toward HIE integration found the number one concern was the availability of safeguards against unauthorized viewing, followed by the ability to review who viewed their data and the ability to select which parts of the medical record are shared (Patel, Dhopeshwarkar, Barron, Sparenborg, & Kaushal, 2012). This showed privacy was a concern from the beginning of NHIN.

More recent studies show that privacy remains a concern. A 2014 Pew Research survey showed people see the most sensitive personal data as the social security number (90% Very Sensitive; 5% Somewhat Sensitive), followed by personal health information (55% Very Sensitive; 26% Somewhat Sensitive) (Madden, 2014). A 2017 study of millennial attitudes toward privacy of health information found the majority (68%) of respondents were concerned about privacy of health information (Pereira et al., 2017). These studies support the idea that privacy of health care information should be one of the primary concerns for stewards of our national health information network.

The Health Insurance Portability and Accountability Act (HIPAA 1996) gave the health care industry the foundation for the protection of electronic patient health information. However, concerns for privacy remain an issue (Palvia, Lowe, Nemati, & Jacks, 2012). HIPAA rules are not uniformly adopted by all states and are not always addressed in the context of an electronic health record. The reason may be there are numerous types of EHR systems and various types (and sizes) of health care settings. Requirements for the privacy of EHR data in a small private practice are barely comparable to those of a large hospital system. Although HIPAA provides general guidance for all provider types, it may not be practical to design state laws with any degree of specificity.

Pam Dixon, executive director of the World Privacy Forum and co-chair of the California Privacy and Security Advisory Board stated, "Consent and sensitive data issues are the first two buttons on the vest. We have to do those first, and if we don't get them right, it doesn't matter what else we do on other issues" (as cited in Raths, 2010, para. 11). Laws must be designed to put the consumer (patient) in control of their electronic health information. For example, there are policies at the federal and state level addressing the use of electronic patient health information for research purposes (Raths, 2010). However, the new landscape of the eHealth Exchange gives access to government, research agencies, and payers alike. There is nothing to control the amount of personal health information that can be collected, stored, and used.

Security

A national network of accessible patient health information inherently creates multiple store points of data. A single server can hold thousands of patient records. Each time a server is accessed by another system, that system acquires a copy of the patient record or some part of it. This leads to data redundancies and protected health information available at various points throughout the network. Any security defect on any part of the network could result in the compromise of hundreds or thousands of records (Farzandipour, Sadoughi, Ahmadi, & Karimi, 2010).

In 2008, the ONC produced a report titled *Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information*. This report outlined eight key principles to "serve as a guide for public and private-sector entities that hold or exchange electronic individually identifiable health information and the development of any compliance and enforcement approaches, including industry self-regulation" (Office of the National Coordinator for Health Information Technology U.S. Department of Health and Human Services [ONC HHS], 2008, p. 4). The key principles are 1) Individual Access, 2) Correction, 3) Openness and Transparency, 4) Individual Choice, 5) Collection, Use, and Disclosure Limitation, 6) Data Quality and Integrity, 7) Safeguards, and 8) Accountability.

The Safeguards principle aligns with HIPAA standards and directly addresses security issues for patient health information: "Individually identifiable health information should be protected with reasonable administrative, technical, and physical safeguards to ensure its confidentiality, integrity, and availability and to prevent unauthorized or inappropriate access, use, or disclosure" (ONC HHS, 2008, p. 9). This principle was codified in HIPAA regulations at 45 CFR 164 Subpart C.

Administrative Safeguards (45 CFR §164.308). Administrative safeguards deal primarily with the day-to-day operations of the health care organization (Adler, 2003). Some of the required standards for administrative safeguards include naming a security officer, conducting risk analysis, maintaining workforce security clearance, and establishing security awareness training. This section also addresses emergency/contingency planning and security incident procedures and reporting. Moreover, this section addresses business associates and how privacy and security standards will apply to those entities under contract that receive, transmit, or otherwise have access to protected health information.

Physical Safeguards (45 CFR §164.310). Physical safeguards include more than the tangible devices and systems that store electronic protected health information. It includes policies and procedures used to access those tangible assets (Alder, 2003). For example, the covered entity must have policies and procedures in place for workstation use and security, back up procedures, and the proper disposal or reuse of electronic devices that store protected health information. Computer rooms and network closets should have physical access control mechanisms that ensure controlled access. Computer workstations should be located or situated in such a way as to reduce any physical access to protected information.

Technical Safeguards (45 CFR §164.312). Technical safeguards follow up physical safeguards for electronic access to patient information. This section addresses standards for password standards, encryption/decryption, unique identifiers, audit control mechanisms and transmission security (Adler, 2003). Furthermore, technical safeguards address person or entity authentication and the authenticity of electronic protected health information.

Interoperability

Although privacy and security are arguably the most concerning problems for the eHealth Exchange, interoperability may be the one confounding factor that creates the greatest barrier to success. Consider the various types of health care providers, various health care settings, various payers and payer systems, and the endless number of electronic software solutions on the market.

It is also important to note the eHealth Exchange is a public-private collaboration, with multiple standards and different technological capabilities (Kibbe & McLaughlin, 2008). Without HL-7 interfacing, many of these systems are unable to communicate at all.

Unique Patient Identifier (UPI). One of the key barriers to interoperability seems to be the development of a Unique Patient Identifier (UPI). There have been different proposals as to how a UPI might be created (Goth, 2009). One idea is to create a system similar to that of the UK and Canada. This would give every person a 10-digit unique number attached exclusively to healthcare information.

Dennis Giokas, Chief Technology Officer of Canada Health Infoway suggested, "designers of US health networks shouldn't try to create national-level identifiers straight off…Regional Health Information Organizations (RHIOs) and Health Information Exchanges (HIEs) should resolve their identity architectures and work outwardly toward other RHIOs and HIEs" (as cited in Goth, 2009, p. 5). Such a system puts identification at the point of HIEs, meaning information at other HIEs would have different identifier conventions. This is very similar to current patient identifiers for medical records at any healthcare organization. This could make the network more secure (as a whole) but still leaves accessibility to question. It would also not resolve redundancies and missing information issues that already exist.

Another patient identification system that seems most practical may emulate that of the current banking system. Online banking systems are already in place and have addressed the issues of privacy and accessibility on a national and international level (Goth, 2009). The health care industry could adopt such standards and make the patient experience as simple and secure as banking online.

Differing data needs. Each key stakeholder has a different set of request criteria and expectations for access. Differences in medical terminology and coding (alone) can hinder accurate and automatic exchange of EHR information (Chen, 2009). Information that satisfies the needs of a radiologist may be very different than that of a researcher. For this reason, certain interoperability must exist to perform specific data mining for the end user. A lack of interoperability standards could be restrictive to some users of health information.

Accessibility

One consideration for accessibility is method of delivery. The eHealth Exchange is designed to provide communications over Internet access. Access is not limited to health care providers. The national network is designed to give access to patients, government agencies, payers, and researchers. Yet, a fully standardized system of delivering electronic health care information on a national level does not exist (in the United States) beyond the capabilities of HIEs and user techniques of faxing and store-and-forward systems (Goth, 2009).

Information blocking. The definition of information blocking is complex but seemingly understood. As stated in an ONC Report to Congress, "information blocking occurs when persons or entities knowingly and unreasonably interfere with the exchange or use of electronic health information" (The Office of the National Coordinator for Health Information Technology [ONCHIT], 2015, p. 8). The experience of information blocking is not new. "While the evidence is in some respects limited, there is little doubt that information blocking is occurring and that it is interfering with the exchange of electronic health information" (ONCHIT, 2015, p. 4).

Although an HIE infrastructure has long been established (The Sequoia Project, 2018), the flow of patient health care information is still hindered. A 2017 Michigan University survey study of 105 HIE leaders found that 95% of respondents were either very familiar or somewhat familiar with information blocking (Adler-Milstein & Pfeifer, 2017). Of greater interest was the primary reasoning given for information blocking; "Our respondents reported that EHR vendors deploy products with limited interoperability and charge providers high fees unrelated to the actual cost to deliver those capabilities or refuse to support information exchange with specific EHRs and HIEs" (Adler-Milstein & Pfeifer, 2017, p. 126).

Conclusion

There seems to be a clear need and a vision for a universal method of accessing patient health information. However, current systems of storing, retrieving, and managing patient information are diverse in design and capability. As the United States continues to move toward a national electronic patient health record, it will be increasingly important to address concerns for the confidentiality, integrity, accessibility, and standardization of electronic patient health information. This paper addressed many of those concerns and presented some additional considerations for further development.

References

Adler, M. P. (2003). Approaching the final security regulations using risk analysis and risk management. *Journal of Health Care Compliance, 5*(6), 10-14.

Adler-Milstein, J., & Pfeifer, E. (2017). Information blocking: Is it occurring and what policy strategies can address it. *The Millbank Quarterly*, *95*(1). https://doi.org/10.1111/1468-0009.12247

Brailer, D. (2004). *The decade of health information technology: Delivering consumer-centric and information-rich health care*. Retrieved from Providers Edge website: http://www.providersedge.com/ehdocs/ehr_articles/the_decade_of_hit-delivering_customer-centric_and_info-rich_hc.pdf

Centers for Disease Control and Prevention. (2017). *Meaningful use*. Retrieved from https://www.cdc.gov/ehrmeaningfuluse/introduction.html

Chen, S. L. (2009). *Achieving effective biosurveillance with the nationwide health information network* (Doctoral dissertation). Retrieved from https://www.proquest.com/libraries/academic/

Exec. Order No. 13335, 69 Fed. Reg. 24057 (2004).

Farzandipour, M., Sadoughi, F., Ahmadi, M., & Karimi, I. (2010). Security requirements and solutions in electronic health records: Lessons learned from a comparative study. *Journal of Medical Systems, 34*(4), 629-42. https://doi.org/10.1007/s10916-009-9276-7

Goth, G. (2009). Unique identifier quandary exemplifies health net obstacles. *IEEE Internet Computing*, *13*(4), 6-10. https://doi.org/10.1109/MIC.2009.92

Health and Human Services Department. (2005). *Consolidated Health Informatics (CHI) Initiative; Health Care and Vocabulary Standards for Use in Federal Health Information*

Technology Systems. Retrieved from Federal Register: https://www.federalregister.gov/documents/2005/12/23/05-24289/consolidated-health-informatics-chi-initiative-health-care-and-vocabulary-standards-for-use-in

Kibbe, D. C., & McLaughlin, C. P. (2008). Health information technology: Strategic initiatives, real progress. *Health Affairs*. https://doi.org/10.1337/hlthaff.27.5.w391

Madden, M. (2014). *Public perceptions of privacy and security in the post-Snowden era. Pew Research Center*. Retrieved from Pew Research Center: Internet & Technology website: http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/

Monegain, B. (2004). HHS: ’The decade of health IT’. Retrieved from https://www.healthcareitnews.com/news/hhs-%E2%80%98decade-health-it

Office of the National Coordinator for Health Information TechnologyU.S. Department of Health and Human Services. (2008). *Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information*. Retrieved from https://www.healthit.gov/sites/default/files/nationwide-ps-framework-5.pdf

Palvia, P., Lowe, K., Nemati, H., & Jacks, T. (2012). Information technology issues in healthcare: Hospital CEO and CIO perspectives. *Communications of the Association for Information Systems*, *30*(19), 293-312. Retrieved from http://aisel.aisnet.org/cais/vol30/iss1/19?utm_source=aisel.aisnet.org%2Fcais%2Fvol30%2Fiss1%2F19&utm_medium=PDF&utm_campaign=PDFCoverPages

Patel, V., Dhopeshwarkar, R., Barron, Y., Sparenborg, J., & Kaushal, R. (2012). Consumer support for health information exchange and personal health records: A regional healthinformation organization survey. *Journal of Medical Systems*, *36*(3), 1043-52. https://doi.org/10.1007/s10916-010-9566-0

Pereira, S., Robinson, J., Peoples, H., Gutierrez, A., Majumder, M., McGuire, A., & Rothstein, M. (2017). *Do privacy and security regulations need a status update? perspectives from an intergenerational survey*. Retrieved from PLOS.org: http://journals.plos.org/plosone/article?id=10.1371/journal.pone.0184525

Raths, D. (2010). The six toughest policy issues: Health IT leaders, and policy-makers grapple with change on several fronts. *Healthcare Informatics, 27*(6), 70-73. Retrieved from https://www.healthcare-informatics.com/article/six-toughest-policy-issues

Speedie, S., & Davies, D. (2006). Telehealth and the national health information technology strategic framework. *Journal of Telemedicine and Telecare, 12*, 59-64. Retrieved from http://journals.sagepub.com/doi/abs/10.1258/135763306778393144

The Office of the National Coordinator for Health Information Technology. (2015). *Report to Congress: Report on Health Information Blocking*. Retrieved from https://www.healthit.gov/sites/default/files/reports/info_blocking_040915.pdf

The Office of the National Coordinator of Health Information Technology. (n.d.). *State Health Information Exchange: State Health Information Exchange Cooperative Agreement Program*. Retrieved from HeatlhIT.gov website: https://www.healthit.gov/topic/onc-hitech-programs/state-health-information-exchange

The Sequoia Project. (2018). What is eHealth Exchange. Retrieved from https://sequoiaproject.org/ehealth-exchange/