10-2013

Data Interoperability and Information Security in Healthcare

Reid Berryman
Western Michigan University, reid.m.berryman@wmich.edu

Nathan Yost
Western Michigan University, nathan.yost@wmich.edu

Nicholas Dunn
Western Michigan University, nicholas.w.dunn@wmich.edu

Christopher Edwards
Western Michigan University, chris.mich.itsupport@gmail.com

Data Interoperability and Information Security in Healthcare

Reid Berryman, Nathan Yost, Nicholas Dunn, and Christopher Edwards
Haworth College of Business
Western Michigan University
Kalamazoo, Michigan 49008
Reid.M.Berryman@wmich.edu
Nathan.Yost@wmich.edu
Nicholas.W.Dunn@wmich.edu
Chris.Mich.Itsupport@gmail.com

Abstract: Interoperability represents the accurate exchange of information and the use of the information for effective decision making. For information exchange to be interoperable, it must be widely interpretable between multiple information systems. At a more granular level, it focuses on the accuracy, consistency and reliability of information exchanged between systems. The healthcare industry has defined many problems when it comes to the best practice of interoperability. Technical, financial, and managerial barriers are present that produce large scale complex problems for the whole industry. Although, a variety of potential solutions have been developed. Some have even been implemented already focusing on semantics, standardization, patient privacy and security. The private and government sectors of the economy have produced new legal and economic incentives, product innovations, along with widely available educational resources that have shown success. Overall improvements will increase quality of care, patient safety, and decrease associated costs across the entire healthcare industry.

INTRODUCTION

Interoperability in its most concise explanation is the ability of systems to exchange information and then use the information exchanged effectively (IEEE, 2013). Problems of systems interoperability are prevalent in the healthcare industry and recent regulatory changes have caused drastic business strategy shifts within the sector. In prior healthcare system implementations, vendor solutions had minimal incentive to standardize any aspects of their Health Information Exchange (HIE) and the information systems they were bound to. Overall, HIE aims to keep records, diagnosis, and treatment integrated between healthcare organizations to ensure patient data integrity along with preventing data loss (Dimitropoulos & Rizk, 2009). Marketplace dominance of specific vendors has caused defacto standardization, bringing a series of unique problems to progress in regard to interoperability, security and the business operations it supports. The need standardized models in systems design for industry technology is being demanded (Association for the Advancement of Medical Instrumentation, 2012). A key success factor brought to light is the cooperation between the practitioners, the industry and the standards bodies (Aylward, Woodhall & Lent, 2007).This preference shift is a result of regulatory compliance and is defining the need for data interoperability with best practice security measures implemented along its side.

Security concerns of the systems design are placed at a much greater priority in the healthcare industry. Privacy concerns with patient data and the high level of risk in the decisions it supports are the important factors to consider. The fear of losing patient information while exchanging data is also a high risk, promoting further importance of all healthcare stakeholders to collaborate (Dimitropoulos & Rizk, 2009). Poor security is a potential symptom of non-standardized systems that communicate. A strong need is recognized from the following perspectives of security: “authorization and authentication, user access, and audit of patient record access and modification, uniform identification of patients, security of data during transmission and at rest (Johnson & Appari, 2008)”. Through market cooperation the overall cost and efficiency of HIE can be improved, producing more timely and accurate information for decision making. From an economic standpoint, there is an untapped source of profit for companies that choose to produce standardized, integrated solutions. With proper implementation of healthcare systems interoperability, industry savings are estimated as large as $77 billion per year (Johnson & Appari, 2008).

When information is truly interoperable, it has the ability to be widely interpretable from a variety of different subjects. Doctors, nurses and all healthcare employees have reached an information access barrier, putting

a threshold on using the information available for effective decision making. The United States (U.S.) Government has promoted interoperable EHR growth through an incentive program, already shown to increase the adoption of comprehensive EHR adoptions since the year 2009 (CDC/NCHS, Nation Ambulatory Medical Care Survey, 2010). See figure 1 in the appendix for a detailed time series graph, comparisons are made between three different EHR criteria. Over half of the reporting health organizations have an EHR/EMR system in use, although only ten percent in the year 2010 have fully functional ones operating with meaningful use.

Data interoperability within healthcare was a problem produced by a variety of discontinuous industry solutions. In the 1970's-1980 the first "practice management" software emerged to increase efficiency (Houston, 2013). No standards existed between vendors that developed this software which required people to reinterpret, input and update data manually between systems. Even if data could be exported, the potential for inaccurate or unreliable information in the transfer process was at high probability. The digital records concept was labeled Electronic Medical Records (EMR) which later on became the conceptual data component of comprehensive Electronic Health Record (EHR) systems. In 2009, the American Recovery and Reinvestment Act (ARRA) included a secondary act called the Health Information Technology for Economic and Clinical Health act (HITECH). HITECH produced a series of financial incentives for health organizations to increase overall EHR system adoption. If "meaningful use" is displayed through a successful audit of fifteen core and five menu set items, the organization is eligible for an incentive payment. More importantly, organizations that choose not to adopt will be financially penalized in the future (Wolf, Harvell, & Jha, 2012, p. 505-513).

Through our research, problems associated with HIE interoperability are categorized, analyzed and discussed while reviewing proposed solutions. Background information was obtained from a variety of accredited sources and specific case studies were chosen for their unique solution proposals of problem areas. Within the two main case study analyses our research teams own understanding, conclusions and recommendations are discussed. Healthcare interoperability is a business objective, so the financial aspects, policies and regulatory changes were reflected in our evaluation as well.

Literature Review

The topic of data interoperability has a short, rapid evolution within the healthcare industry. As recent as 2006, fewer than 10% of hospitals in the United States had a full intergraded Electronic Medical Record (EMR) system (Smaltz, D. H., & Berner, E. S, 2007). An EMR by itself displays patient data normally found in a "paper chart", used for diagnostic processes (Healthit.gov, n.d.) EMR represents the first major product of change when healthcare organizations switched to digital systems. EMR's were of the first technical components within healthcare representing major issues of interoperability. Technical standards have been created from an information systems perspective, although the variety of standards used still leaves interoperability issues with communication. The technical standards created were at first divided on an international basis. Many European countries have enforced technical standards for their information systems, such as those developed by the European Committee for Standardization (CEN). Health Level Seven (HL7) is an international healthcare informatics interoperability standards body popular with regulation changes in the U. S. Although, the standards set in place by HL7 still do not fall under "open standards" but their specifications as of 2002 have been placed into the public domain (wiki). Furthermore HL7 in 2012 decided to promote interoperability within the healthcare industry through the release of most of its intellectual property (IP). HL7 previously operated under a licensing model that required businesses that used its standards to license them at a fee. This recent choice landmarks an important issue, as HL7's standards are viewed as defacto in much of the industry. After releasing their IP, a large component of their research and business will be available for use for free. This will potentially influence greater competition in the market place for software, hardware and technical solution vendors. The reduced barrier of implementation will result in greater quality of care and reductions in cost overall for providers. These two factors directly influence the adoption rate within the marketplace, offering a large positive change for interoperability in healthcare.

The issue of interoperability within the United States healthcare system is one of a half implementation. The topic of "semantic interoperability" is a specific reason issues of incompatibility arise. Syntactic standards exist from a purely technical point of view, although the lack of semantic compatibility causes problems of definition when data is being interpreted. Sematic interoperability is best defined as "Ability of a system or a product to work with other systems or products without special effort on the part of the customer. Interoperability is made possible by the implementation of standards."(IEEE, 2013). This issue in itself promoted the creation of EHR systems, which poses unique advantages over simpler EMR based systems. EHR systems are designed with interoperability as a focus, so EMR's are often used as data source for EHR systems. The difference between the two is important, as

they serve different purposes within the healthcare IT industry. A primary difference between them is the scope of EHR. EHR systems are designed to share patient data between health care providers. A clear definition was made by The National Alliance for Health Information Technology (NAHIT) as data that "can be created, managed, and consulted by authorized clinicians and staff across more than one healthcare organization." (Healthit.gov, n.d.) The overall goals of EHR are directly correlated with the goals of an interoperable HIE for patient data. Direct benefits of secure access to the latest information for patients are clear. Healthcare providers are businesses that rely on fast interpretation of accurate data to perform their duties most effectively. Effective EHR implementation ensures specifics such as an individual's recent life threatening health changes, clinician's notes and updated lab results are securely accessed and universally interpreted

Statistical data from 2009 detailing the use of comprehensive EHR systems shows a low actual adoption rate. Only 1.5% of hospitals have comprehensive EHR systems, due largely to concerns of cost, technical support and physician resistance (Massachusetts Medical Society, 2009). Recent U. S. legal regulatory changes are directed at increasing this adoption rate. The HITECH act was signed into law shortly after this adoption rate statistic was produced in 2009. The goal is to ensure the proper implementation of EHR systems through economic incentives, if the outlined government criteria are met by providers. HITECH provides a three stage initiative, with data interoperability as the core method and tool of overall improvement within the health care industry. In stage one, providers must digitize all records and regularly use digital records for care decisions. Stage two is where interoperability is first introduced; organizations must show they can "share records with other providers, regardless of the EHR systems in use." Stage three represents the final goal of "meaningful use", representing a positive social externality globally. Stage three will allow better understanding of the large amounts of data collected through the use of analytics. Analytics allows for the ability to "learn from the electronic information" through data mining and other statistical computations (Blumenthal, M.D., M.P.P., 2011).

Healthcare providers take part in semantic interoperability with the use of phone, fax, email, hardcopy and, in some cases, electronic exchange. Without these communication methods, specialist referrals and procedure scheduling would be a much more difficult operation. Modern semantic interoperability requires time resource constraints and is affected by latency issues with high error probability. This is in part is due to the multiple avenues of sending information. Partners in the healthcare system use a variety of access media and delivery methods. This inconsistency in their choice to send and receive information often results in information duplication. Another pitfall of varying access media and delivery methods is the unaccountable lost information during the transportation and interpretation process. Data loss remains one of the greater symptoms of non-interoperable systems (Bass, & J P Systems, Inc., 2011).

Beyond the medium the message is delivered in, the actual message can change from partner to partner. Various participants in healthcare have created systems of communication amongst themselves. Synonyms and homonyms can cause a great deal of problems between healthcare providers and their partners. A single provider may go into great detail concerning a procedure or process; whereas another has minimal information about the same procedure or process. Organizations in general may use the same name or phrase between different functional processes. Some terms may be incorrectly interpreted between providers for the same symptom, disease, illness, etc. Deciphering the terminology varying providers use and aggregating them into a standardized library is a difficult technical and managerial task. Implementation would have to work through push back from industry employees, whom may be unwilling to adapt to new terms or have issues of understanding during the changeover process (Healthcareinteroperability, 2011).

On the technical side, the matching and mapping of terms can be broken down into multiple levels as well. Technical problems within semantics and syntactic design can be classified in four main area of heterogeneity. Syntactic heterogeneity comes about with differences in the language used for representing the same elements. Structural heterogeneity shows differences in the types of element structures. Model and representational heterogeneity explains the differences in database models (i.e. Relational, Object-oriented, RDF, OWL, etc.). Semantic heterogeneity defines how the terms are represented. (Nagarajan, Verma, Sheth, Miller, & Lathem, 2006). These well classified problems of semantics within the industry are the first step to obtaining solutions. By breaking the semantic and syntactic issues down into manageable levels, solutions can be created much more timely and reliably.

The next task, with the integration of terms and definitions to a standardized form, is the relation of the technical syntax to the semantic meaning. Using the proper syntax ensures the structure of information will remain intact, but there is no guarantee it will be understood universally by all parties. Web-based programming languages represent this same concept; any computer that uses the internet is able to interpret the structure of the information sent to it. However, if pages displayed are created in a foreign language, a viewer unfamiliar with that language will have interpretation problems. Semantic interoperability of person to person communication makes certain the

message is understood by the parties sending and receiving messages. Documents need to be created with standardized structure and terminology implicit to professionals in the medical field, leaving no question as to the purpose of the message communicated. A final measure in addressing problems of semantics is the creation of computable semantic interoperability. Ensuring proper delivery of straight-forward messages via electronic media used to make appropriate decisions based on the meaning contained. (Mead, n.d.). The human interpreter is the last component of the communication process. If all technical errors and standardization of the information are solved, the scope to which interoperability represents the problem has at least reached its technical boundary.

The U.S. Governments incentivized push for hospitals and medical treatment facilities to convert to comprehensive EHR systems has caused concern for the security of patient's medical records. With the variety of non-interoperable system structures, often raw data of unsecured exports are the only means of interpretation. Once in an unsecured, unaccountable exported format, the risk a privacy breach is drastically increased. In the final ruling for the modifications to the "HIPAA Privacy, Security, Enforcement, and Breach Notification Rules" these concerns were addressed (U.S. Department of Health and Human Services, n.d). Security has been an issue since the conception of the idea for EMR's and many statistics of breaches and problems have been well documented. In 2012, there were 154 breaches reported with 2,237,873 records lost in those breaches (Identity Theft Resource Center, 2012). The records lost, manipulated or accessed by unauthorized individuals constituted as 13% of the medical records stored by compliant reporting health agencies nationwide.

The government and military have been using EMR's longer than the general populace due to rapid and frequent movement of soldiers internationally, along with the greater risk of heath adverse situations they may encounter. Problems of interoperability and personal health information (PHI) breaches were first experienced within this sector and on person hardcopy backups were frequently ruined from environmental conditions. In addition, medical records in a physical format can be altered with no secure measure of accountability. With this thought in mind the U.S. Military started the Composite Health Care System (CHCS) in 1988. This was developed in hopes of keeping medical records intact, correct, and readily available. CHCS was combined with the Armed Forces Health Longitudinal Technology Application (AHLTA) which made it easier for doctors to add notes into medical records without having to access the entire record. This Military program has been an inspiration for the civilian health care sector to follow suite. Although no implementation has remained risk and breach free, TRICARE, the Department of Defenses (DOD) health care program has reported over 4.9 million records were compromised in a single incident (Mearian, 2012). Prior to EMR, health professionals requiring access to an individual's medical record had physical restrictions and time constraints as influencing factors. With the removal of these two factors through advancements in technology, the balance between security and convenience must be properly aligned. An example of a technology involved in this balance is Radio-frequency Identification (RFID). A company based out of Florida in 2008 started the controversial practice of offering implanted RFID in patients who requested and consented to the outpatient surgery (Business Wire, 2008). This device is about the size of a grain of rice and can be read electronically to obtain medical record and emergency contact information. Quicker access to a patient's medical information is the advantage, although it also gives this information to anyone with an RFID reader. Identity theft cases have been previously documented in cases of RFID credit fraud, so the same concerns for privacy of health records exist with these RFID implants.

In the Final Ruling of the HITECH for the adjustment of HIPAA, there are several new definitions and connections between any organizations involved in the transfer of patient medical information. Any Health Information Organization (HIO) that handles patient medical information on a regular basis have been reclassified as "business associates" and are accountable for information loss or breach that occurs (Gajanayake, Iannella, & Sahama, 2011). The creation of accountability for incidents promotes safer access overall, although specific technical requirements preventing data loss or attacks are absent. The updated polices in HIPAA and HITECH act largely just increase the penalty for incidents and promote a more stringent reporting procedure. The lack of outlined specifics is a burden the HIO management must handle and is also left up to individual companies providing certified EHR systems.

Analysis and Observation

From our research, the advantages of Interoperability are quite clear from a purely technical perspective. Although considerations of all variables and constraints a business operates under must be accurately evaluated to determine the benefits offered. By technical definition, Interoperability allows uniform integration and communication of information systems. Advantages derived from interoperable systems working together must also be recognized for the malicious aspects created in the process. Malicious code spreads well within environments that are predictable,

assessable, and interconnected. These three advantages can very well also become advantages of adversarial operations. If a hospital has a standardized and interconnected environment, greater security responsibilities are a burden of the business. When the security of the infrastructure and polices are not aligned, the advantages of interoperability are quick to be lost at the expense of the risk it produces. Through our research, the cost benefit of implementing government certified interoperable EHR suites must be justified alongside the security budget of the organization. This relationship is a common tradeoff when a business chooses to upgrade or add new technology to their operational model. When new technology is implemented, new and unique problems also arise alongside it.

The financial component of businesses is the primary reason a business can continue to exist. Without positive net income, operations cease and the institutions can no longer justify their continued existence. The U.S. Government understood healthcare cost driven objectives well when in 2009 the American Recovery and Reinvestment Act (ARRA) was passed subsequently including the HITECH act. HITECH produced a series of financial incentives for health organizations to increase overall EHR system adoption nationwide. If "meaningful use" is displayed through a successful audit of fifteen cores and five menu set items, the organization is eligible for an incentive payment. More importantly, organizations that choose not to adopt will be financially penalized in the future. With the economic incentives, a relationship is shown when communicating the value in a nationwide HIE. By the U.S. Government offering immediate return on investment, the cost justification for each individual business was greatly persuaded. The comprehensive EHR system adoption rate statistics are the most influential key performance indicator available when measuring the effectiveness of the HITECH program. The adoption rate continues to increase, although as outlined in HITECH, the momentum created by incentive payments may not last in its current outlined state. The payments began in 2011 and will continue to offer a payout for the next five years, but after this time period actual penalties will be incurred. The incentive payment structure is outlined in figure 2 of the appendix. The penalties original intention is to push hesitant HIO's to adopt, although the actual number of these has yet to be determined. Thus, a nationwide HIE loses its effectiveness if an exponential increase is not represented in a timely manner (Centers for Medicare and Medicaid, 2013).

Case Study and Discussion

Our industry research performed brought about two main categories of problems in relation to interoperability within healthcare. The first area discussed contains perspectives from the technical and fundamental focuses when reviewing semantic problems of information exchange. The second problem area addressed is the security and privacy concerns of patient records in a comprehensive interoperable system environment. Each of these two core problem areas were analyzed with a prior case study focused in the aforementioned specific problems. Each core problem area of interoperability is further discussed and defined within the scope of the case study they derived from. After proper definition is given to the problem area, the solutions are discussed and analyzed.

The issue of semantics is a primary task in solving overall communication problems of interoperability between EHR systems. HL7 is a standards body that has released effective technical whitepapers and resources on their widely used protocols and data models. Their framework is a potential overall solution to many of the technical problems experienced within HIE. The request for standardization is easy to create, but forming a government team responsible for its oversight requires resource planning and time. With the release of HL7's standards into public domain, focus has been given at implementing their defacto standards as true standardization following all of HITECH and HIPAA regulatory principals (Health level Seven, n.d).

In the case study "Semantic Interoperability of Web Services - Challenges and Experiences" HL7's publically available standards are discussed from an "ontological" perspective (Mendes, & Rodrigues, 2011, p. 1). The study describes the "semantic web" in relation to the widely discussed interoperability issues within healthcare EHR systems. The authors propose a contrasting view to other industry solutions. The analyses determined interoperable semantic issues are best solved by restraining from hard coded strict standards. A focus on the use of "model-based" specifications for EHR system design is discussed. In the studies model-based approach, a strict representation to promote full interoperability would exist, while remaining open enough to allow updates and revisions over time. This primary distinction separates this specific study from more common recommendations of centralized vocabulary databases, which are still discussed as a supplemental solution.

Through the design of these models, benefits of interoperability are further explained. Attaining the design and definition middle ground of the proposed HL7 based models will allow true integration of future software updates. This function based methodology is called Service-oriented Architecture (SOA) and industry wide adoption of such design methods could promote a drastic increase with interoperable software and hardware brought to

market. A root of the interoperability problem is the vendors who design and create solutions sold to health organizations. If their product design process can be influenced, the phased software and hardware upgrades will eventually fade out non-interoperable components (Mendes, & Rodrigues, 2011).

Every implementation of a solution brings unique and different problems forward. Within the systems development lifecycle, it is common for security to be implemented in a post-facto manor. Although, post-facto implementation goes against best practice principals of system design and information security. The scope size and investment risk at stake in the healthcare reform finds post-facto security as an unacceptable practice. Security and privacy concerns have been discussed greatly from top to bottom approach, forming policy and regulations to guide the reformation process. The HITECH act brought forward updated regulations for security and privacy guidelines within HIPAA. The case study "Sharing with Care" discusses "information accountability" as an effective security and privacy strategy to follow new outlined regulatory requirements (Gajanayake, Iannella, & Sahama, 2011). Furthermore, the study focuses on "privacy by design", a direct solution to post-facto security implementation. A proposal is made that if e-health systems are designed around proper methodologies, patient privacy will actually increase. Many websites collect general and medical information through consumer ignorance of data tracking. Consumers unknowingly waive and reveal potential ailments through publically available diagnostic sites that operate legally with debatable ethics. Data ownership of the individual is an increasing request as more information is stored in cloud based infrastructures. In healthcare, the accessibility of personal health records (PHR) is the classification term to represent this data. As for patient privacy, the problem is therefore best defined as one of accountability. Websites utilizing data mining techniques which then sell market research data are not required to be accountable for the freely available information they collect. If consumers had options of using a regulated service, with their personal standardized records this business model would prove less effective. In the updated HIPAA regulations, HIO's are required to "provide access in electronic format" which promotes the aforementioned principles. (Blumenthal, M.D., M.P.P., 2011). Prior to this regulation, this level of patient access would likely not have been implemented in EHR systems. The ability a customer to access PHR's anywhere and anytime is significant from a compatibility standpoint as well. Providers that forgo the economic incentive and receive penalties would still be able to view PHR's produced by compliant organizations. Thus, this regulation promotes a global positive externality and benefits the public quality of healthcare for all individuals.

As determined in earlier analysis and observation, addressing privacy concerns of PHR's is an influential point in overall adoption. Specific policy has not been standardized for the measures each health organization must put in place. Instead, reasonable efforts must be made by the business to protect patient data. This study addressed the concept of accountability from a top down approach to provide overall security. Accountability within EHR systems were divided into three factors. The "identification of accountable parties, issues a party is accountable for and the appropriate mechanisms for accountability make up the accountable best practices of a certified EHR system" (Gajanayake, Iannella, & Sahama, 2011). The first factor, identification of accountable parties, is best explained as a classification and segregation process. Through categorization, the parties' level of access can be determined. The goal of secure information access is achieving the proper level of access and ensuring the correct access is given to perform a specific task. Understanding what constitutes as a privacy invasion is an important activity to define as well. If a doctor, technician or any other employee has no purpose for accessing a record and they do, a breach in privacy has occurred. The process and components of how a proper accountability mechanism works are displayed in figure 3 of the appendix. Identifying the information requested along with the information seekers required level of access leads to proper privacy protection. With proper accountability tracking, violations could be tracked and proper discipline and penalties of an individual addressed.

Conclusions and Recommendations

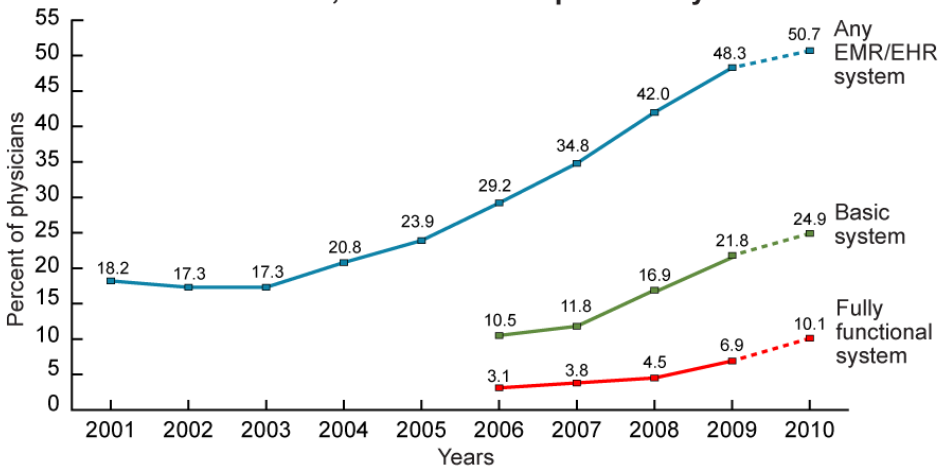
Interoperability represents a vital and core focus of the modern healthcare reform. Understanding why it is a problem can continue to be analyzed at an ever more granular level. If the government incentive program for healthcare organizations is able to drive the expected results, numerous positive benefits will be gained domestically and globally. The financial gain of properly implemented HIE is not derived from new and profitable income, but instead directed at cutting the overhead costs, saving time, and preventing waste from an operational standpoint. When the entire healthcare industry experiences cost reduction, the government related programs also experience benefit. Programs such as Medicare and Medicaid will require less funding to sustain their current operations, reducing the contribution to the overall United States deficit. This economic reform technique known as "cost-shifting", showcases a unique and rapid approach to changing an entire industry. At a worldwide economic level, the movement of interoperable systems within healthcare promotes great overall positive change. The government in

many ways also operates like a business and it clearly sees the return on investment capable in a nationwide HIE project.

In addition to our economic based conclusion's, the security and privacy aspects of a nationwide HIE were researched and analyzed. The concerns discussed specifically with interoperable systems were found to hold much less weight than added benefits of security and accountability created. The current design methodologies driving nationwide HIE are in depth, and vendors are taking due consideration from the initial design phases to incorporate security, accountability and standardized semantic meaning in new hardware and software. Furthermore, the incentives offered by the government are only for certified EHR systems. Government certified software promotes EHR vendor competition and quality control for software design influence. In the event a security exploit exists, the issue can be tracked, understood and resolved much quicker than in dispersed information system islands. From a privacy standpoint, the non-interoperable EHR systems in use offer almost little or no accountability. If a practitioner or anyone in the office wants to access information on a patient, they may do so whether it is relevant or not. A nationwide HIE will include strong aspects of accountability as a security measure for privacy. Whenever a specific record is accessed, the patient will be in complete control of knowing who accessed their record, when it was accessed and why. If the record was improperly accessed or maliciously accessed, the accountability is present to discover who is at fault for the breach. While this may not stop patient record privacy breaches, the ease of traceability certainly produces valuable follow up information to solve future problems (Gajanayake, Iannella, & Sahama, 2011).

APPENDIX

Figure 1. Percentage of office-based physicians with electronic medical records/electronic health records (EMRs/EHRs): United States, 2001–2009 and preliminary 2010



NOTES: Any EMR/EHR is a medical or health record system that is either all or partially electronic (excluding systems solely for billing). The 2010 data are preliminary estimates (as shown by dashed lines), based only on the mail survey. Estimates through 2009 include additional physicians sampled from community health centers; prior 2008 combined estimates were revised to include those physicians (4). Estimates of basic and fully functional systems prior to 2006 could not be computed because some items were not collected in the survey. Fully functional systems are a subset of basic systems. Some of the increase in fully functional systems between 2009 and 2010 may be related to a change in survey instruments and definitions of fully functional systems between 2009 and 2010 (see Table for more details). Includes nonfederal, office-based physicians. Excludes radiologists, anesthesiologists, and pathologists.
SOURCE: CDC/NCHS, National Ambulatory Medical Care Survey.

Figure 1: (CDC/NCHS, Nation Ambulatory Medical Care Survey, 2010)

Maximum Incentive Payments for Medicaid EPs Who Are Meaningful Users in the First Payment Year							
		Medicaid EPs who begin MU of certified EHR technology in					
		2011	2012	2013	2014	2015	2016
Calendar Year	2011	$21,250					
	2012	$8,500	$21,250				
	2013	$8,500	$8,500	$21,250			
	2014	$8,500	$8,500	$8,500	$21,250		
	2015	$8,500	$8,500	$8,500	$8,500	$21,250	
	2016	$8,500	$8,500	$8,500	$8,500	$8,500	$21,250
	2017		$8,500	$8,500	$8,500	$8,500	$8,500
	2018			$8,500	$8,500	$8,500	$8,500
	2019				$8,500	$8,500	$8,500
	2020					$8,500	$8,500
	2021						$8,500
	Total	$63,750	$63,750	$63,750	$63,750	$63,750	$63,750

Figure 2: (Mullin, & Hitechanswers.net, 2011)

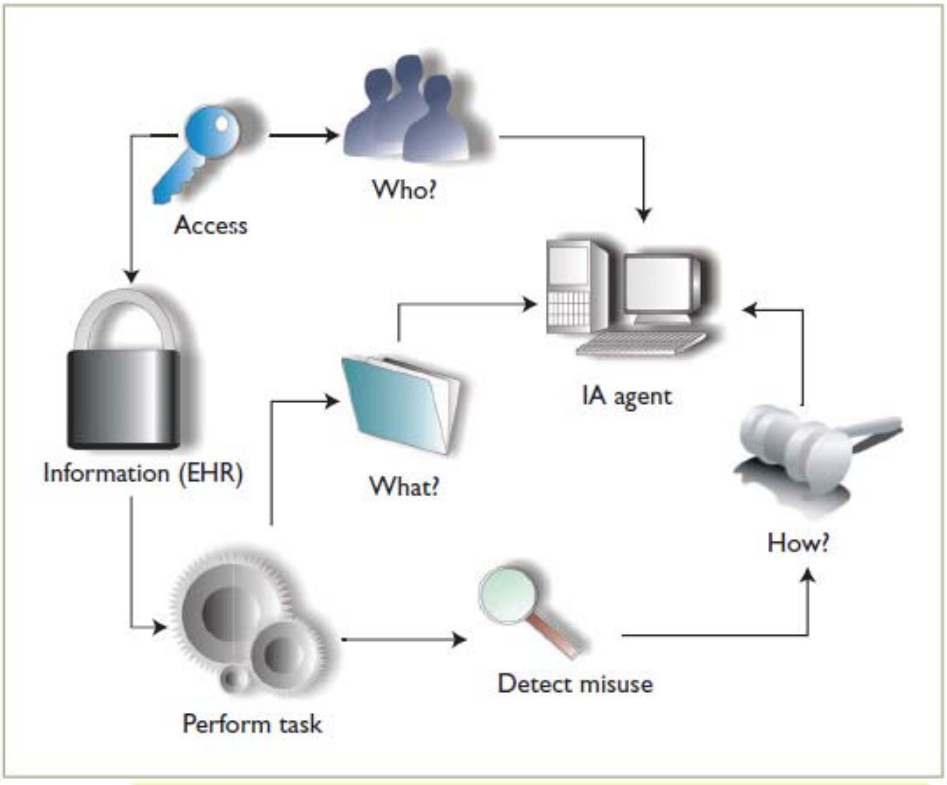


Figure 3: (Gajanayake, Iannella, & Sahama, 2011)

REFERENCES

Association for the Advancement of Medical Instrumentation. (2012). Aami white paper.*Medical Device Interoperability*, 13-16. Retrieved from http://www.aami.org/interoperability/Materials/MDI_1203.pdf

Aylward, D., Woodhall, J., & Lent, B. (2007). Disaster resource guide. *Facing The Challenge Of Data Interoperability* , 148. Retrieved from http://www.disaster-resource.com/index.php?option=com_content&view=article&id=335:facing-the-challenge-of-data-interoperability&catid=9:crisis-response&Itemid=15

Bass, D., & J P Systems, Inc. (2011). Listening- One of the Hardest Parts of Healthcare Interoperability Requirements Gathering. Retrieved from http://www.healthcareitinteroperability.com/docs/JPS%20article_listening_ver2.pdf

Blumenthal, M.D., M.P.P., D. (2011). Implementation of the Federal Health Information Technology Initiative. *The NEW ENGLAND JOURNAL of MEDICINE*.

Business Wire (2008, April). *VeriChip Corporation Launches HEALTH LINK SYSTEM in Florida Revolutionizing Future of Emergency Medicine | Business Wire*. Retrieved April 2013, from http://www.businesswire.com/news/home/20080429005913/en/VeriChip-Corporation-Launches-HEALTH-LINK-SYSTEM-Florida

CDC/NCHS, Nation Ambulatory Medical Care Survey (2010, January). Figure 1. Retrieved from http://www.cdc.gov/nchs/data/hestat/emr_ehr_09/emr_ehr_09_fig1.png

Centers for Medicare and Medicaid (2013, April). *EHR Incentive Programs - Centers for Medicare & Medicaid Services*. Retrieved April 2013, from http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/index.html?redirect=/ehrincentiveprograms/

Dimitropoulos, L., & Rizk, S. (2009). Health affairs. *A State-Based Approach To Privacy And Security For Interoperable Health Information*, *28*(2), 428-434. doi: 10.1377/hlthaff.28.2.428

Gajanayake, R., Iannella, R., & Sahama, T. (2011). Sharing with Care An Information Accountability Perspective. *IEEE Computer Society*, 31-38. doi:1089-7801/11/

Health level Seven (n.d.). *HL7 - FAQs - Free IP*. Retrieved April 2013, from http://www.hl7.org/about/faqs/freeip.cfm

Healthcareinteroperability (2011). Retrieved April 2013, from http://healthcareinteroperability.com/datamapping.html

Healthit.gov (n.d.). *Definition and Benefits of Electronic Medical Records (EMR) | Providers & Professionals | HealthIT.gov*. Retrieved April 2013, from http://www.healthit.gov/providers-professionals/electronic-medical-records-emr

Houston, N. (2013, January). History of Electronic Health Records (EHR) | A Timeline of EMR History [Web log post]. Retrieved from http://blog.softwareadvice.com/articles/medical/ehr-timeline-113

Identity Theft Resource Center (2012). *2012 Data Breach Stats*. Retrieved from http://www.idtheftcenter.org/ITRC%20Breach%20Stats%20Report%202012.pdf

IEEE (2013). Standards glossary. In IEEE Retrieved from http://www.ieee.org/education_careers/education/standards/standards_glossary.html

Johnson, E., & Appari, A. (2008). Information security and privacy in healthcare: Current state of research. 14-15. Retrieved from http://www.ists.dartmouth.edu/library/416.pdf

Massachusetts Medical Society (2009). Use of Electronic Health Records in U.S. Hospitals.*New England Journal of Medicine*. Retrieved from http://www.nejm.org/doi/full/10.1056/nejmsa0900592

Mead, C. N. (0). Data Interchange Standards in Healthcare IT—Computable Semantic Interoperability: Now Possible but Still Difficult, Do We Really Need a Better Mousetrap?.

Mearian, L. (2012, August). *'Wall of Shame' exposes 21M medical record breaches - Computerworld*. Retrieved April 2013, from http://www.computerworld.com/s/article/9230028/_Wall_of_Shame_exposes_21M_medical_record_breaches

Mendes, D., & Rodrigues, I. (2011). A Semantic Web pragmatic approach to develop Clinical ontologies, and thus Semantic Interoperability, based in HL7 v2.xml messaging.*Universidade de Évora*.

Nagarajan, M., Verma, K., Sheth, A. P., Miller, J. A., & Lathem, J. (2006). Semantic Interoperability of Web Services - Challenges and Experiences. doi:10.1109/ICWS.2006.116

Renner, S. A. (2001). In: Federal database colloquium '01.*A "Community of Interest" Approach to Data Interoperability*, &-&. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.127.4491&rep=rep1&type=pdf

Solomon, M. (2006). Regional health information organizations: A vehicle for transforming health care delivery?. *Springer Science Business Media,*, 31:35-47. doi: DOI 10.1007/s10916-006-9041-0

Smaltz, D. H., & Berner, E. S. (2007). The executive's guide to electronic health records. Health Administration Press.

U.S. Department of Health and Human Services (n.d.). HIPAA Privacy, Security, and Breach Notification Audit Program. Retrieved April 2013, from http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/

Wolf, L., Harvell, J., & Jha, A. (2012). Hospitals Ineligible For Federal Meaningful-Use Incentives Have Dismally Low Rates Of Adoption Of Electronic Health Records. *Project HOPE*, *31*(3), 505-513. doi:10.1377/hlthaff.2011.0351