A Viewpoint of Security for Digital Health Care in the United States: What's There? What Works? What's Needed?

Steven A. Demurjian, Department of Computer Science and Engineering, University of Connecticut, Storrs, CT, USA

Alberto De la Rosa Algarín, Department of Computer Science and Engineering, University of Connecticut, Storrs, CT, USA

Jinbo Bi, Department of Computer Science and Engineering, University of Connecticut, Storrs, CT, USA

Solomon Berhe, Department of Computer Science and Engineering, University of Connecticut, Storrs, CT, USA

Thomas Agresta, Department of Family Medicine and the Center for Quantitative Medicine, University of Connecticut Health Center, Farmington, CT, USA

Xiaoyan Wang, Department of Family Medicine and the Center for Quantitative Medicine, University of Connecticut Health Center, Farmington, CT, USA

Michael Blechner, Department of Pathology and the Center for Quantitative Medicine, University of Connecticut Health Center, Farmington, CT, USA

ABSTRACT

In health care, patient information of interest to health providers, researchers, public health researchers, insurers, patients, etc., is stored in different locations via electronic media and/or hard-copy formats. All potential users need electronic access to health information technology systems such as: electronic health records, personal health records, patient portals, and ancillary systems such as imaging, laboratory, pharmacy, etc. Controlling access to information from multiple systems requires granularity levels of privileges ranging from one patient to a cohort to an entire population. In this paper, we present a viewpoint of the state of secure digital health care in the United States, focusing on the resources that need to be protected as dictated by legal entities and regulations, the available approaches in the present state-of-the art, and, the potential needs for the future of security for digital health care. By utilizing a real world scenario, the authors explore the limitations of health information exchange in the United States, and present one possible architecture for secure digital health care that builds on existing technology alternatives.

Keywords: *Digital Health Care, Electronic Health Records, Health Information Exchange, Health Information Technology, Security*

DOI: 10.4018/ijphim.2014010101

1. INTRODUCTION

Over twenty years ago, two articles related to health care security were published that were noteworthy for the time. In (Biskup, 1990), privacy and confidentiality in medical information systems was explored, advocating a role-based approach, and detailing the state-of-the-art in available systems. In (Ting, 1990), a case study of mental health delivery from information and semantic perspectives was presented, providing scenarios of usage of information by physicians, nurses, etc., and promoting a role-based approach as the most appropriate solution. What is surprising is what has stayed the same and what has changed over the last 20 plus years in the health care domain in terms of tracking patient care (via paper or electronic form) and facilitating secure information exchange as a patient transitions between care settings, more specifically in the United States. For instance, in 1990, would anyone have predicted the introduction of the Health Insurance Portability and Accountability Act[1] of 1996 (HIPAA) Privacy and Security Rules for protected health information? At the time, health care delivery was based more on paper than electronic health records (EHRs). How about the Genetic Information Non-discrimination Act (GINA)[2] of 2008? GINA aims to protect a patient's genetic information against discrimination in health insurance and employment. Or even the Ethical, Legal and Social Implications (ELSI) research program? ELSI was introduced to manage genomic data for personalized medicine. There have also been dramatic changes in patient care, including: EHRs in some medical doctor offices ("implementation rates reached 68% in family practices in 2011"[3] while "just 27% of physicians used EHRs with multi-functional capabilities"[4]); and, personal health records (PHRs) for patients to store their own health information (and download medications from a pharmacy, share data with providers, etc.). Evolving needs for health care delivery include a Patient Centered Medical Home[5] where one provider coordinates care for patients with chronic diseases; an accountable care organization (ACOs)[6] to coordinate providers regarding Medicare patients with chronic conditions; and the upcoming Meaningful Use Stage 2[7] capability for patients to be able to view, download, and transmit their records which will require the development of a standardized transmission of all types of medical information. These three and other evolving initiatives will require secure data collection from multiple health information technology (HIT) systems.

The harsh realities in health care and HIT adoption in the United States are: the limited capabilities of health information exchange (HIE) among all of these various data sources; the high number of providers that are predominately paper based with limited or no access to EHRs or other HIT systems; and, the fact that security is often an afterthought in this process, supported for individual systems for specific providers, but overlooked when one attempts to bring together patient data from multiple electronic sources. In patient centered medical homes, the effective care of a diabetes patient with high blood pressure may involve the family practitioner (who sees the patient regularly), an endocrinologist (if diabetes is complex in its manifestation), a cardiologist (diabetes patients often have heart disease), and a nutritionist (for managing diet or dealing with obesity). These four providers may have different EHRs (or none) and an inability to share data (patient history, lab test results, etc.) to facilitate the required care. The access needs to be integrated (electronic sources), secure (individual sources and across the integrated sources), and collaborative (individuals can view/update same patient record simultaneously). Our main objective in this paper is to enumerate prevalent issues for secure, integrated, and collaborative health care in the United States, requiring us to provide a roadmap for secure digital health care in the not so distant future. Our viewpoint is intended to answer questions such as: what patient information is available for each source, how can information be standardized for ease of use and exchange, how is the local security for that source managed, what needs to be protected from each source, is there a global security policy across the integrated sources, and what security methods are appropriate to employ.

The remainder of this paper has five sections. Section 2 presents background security for digital health care and the involved health information technology systems by focusing on existing United States laws, standards, and emerging models of care spanning clinical, genomic, and phenotypic information. Section 3 provides a scenario on the actual experiences of one co-author in navigating the United States health care system with HIT in use at some level by most providers, but with paper-based records still exchanged via snail mail and fax. Section 4 details a proposed security framework that considers all of the constituent elements of information exchange in the United States, with examples of HIT systems, standards, and applications, as well as their interactions. Using this as a basis, Section 5 proposes a core set of recommendations organized by area that represents our viewpoint of what must be supported for security for digital health care. Finally, Section 6 concludes the paper, and in the process, addressed the applicability of the work herein to other regions of the world.

2. SECURITY FOR DIGITAL HEALTH CARE AND HEALTH INFORMATION TECHNOLOGY

Security for digital health care goes well beyond the needs of compliance of HIPAA, which provides a set of security guidelines in the usage, transmission, and sharing of protected health information. In addition, there is a need to: protect personally identifiable information, including names, addresses, accounts, credit card numbers, etc.; encrypt protected health information and personally identifiable information data and its secure transmission (e.g., using SSL); extensive usage of standards for storage and exchange (Health Level Seven's Clinical Document Architecture[8] and the Continuity of Care Record[9] for administrative, patient demographics, and clinical data); leveraging a wide range of health care standards (e.g., LOINC[10], SNOMED[11], UMLS[12]); and, dealing with data interoperability issues for health information technology systems that use a wide range of data formats (e.g., XML[13], RDF[14], JSON[15], etc.). Instead, to attain security for digital health care in the United States, we will need all of these underlying technologies and standards coupled with a strong understanding of the way that health care data is utilized by the different stakeholders. We must also include the emerging need to manage genomic data for personalized medicine and its potential future integration and/or consolidation with EHRs via ELSI, which is tied to GINA. GINA protects a patient's genetic information against discrimination in health insurance and employment, including: genetic test of patient, his/her family members, fetus of individual or family member, family medical history, and request/receipt of genetic services that may include research trials. HIPAA's rule insures that protected health information is securely maintained with patients retaining rights to their information stored in a personal health record (patient controlled), or to access information from a provider's record (EHR or hard copy). While HIPAA provides guidelines for this, it is important to note that it also allows entities to disclose the information under certain situations. HIPAA's rule defines the "series of administrative, physical, and technical safeguards for covered entities to use to assure the confidentiality, integrity, and availability of electronic protected health information". For ELSI, protection of information must be reconciled across HIPAA and GINA to securely deliver the combination of clinical, genomic, and phenotypic information to researchers, clinical providers, support personnel, insurers, and patients.

Security for digital health care transcends just protecting the information, and must strongly consider the usability of the information by a wide variety of stakeholders using a broad range of HIT systems to effectively and securely leverage different types of patient data, including:

- EHRs (e.g., Allscripts[16], GE Centricity[17], VistA[18], etc.), which are electronic repositories of patient medical records that may exist in provider offices, clinics, and hospitals.
- Personal health records (such as Microsoft HealthVault and webMD) that allow patients to manage their own health care data.
- Patient portals (often part of EHRs) that allow patients to electronically request appointments, prescription refill requests, arranging a referral to another provider, etc.
- Personalized medicine health portals such as Genomas[19], which allows providers to view their own patients' genetic data against their medical record (EHR) in order to bridge the gap between providers and medical researchers.
- Ancillary systems for laboratory results (e.g. blood work), evaluating X-rays, MRIs, CT Scans, etc. to be electronically delivered to providers, pharmacy systems for tracking medication and interactions, etc.
- Patient applications for access to education information and management of chronic diseases, medications, and interactions with providers.
- A clinical research data warehouse that contains de-identified clinical data loaded from medical records for patients with permission to have their data used for medical research, or for public health researchers to do population studies.

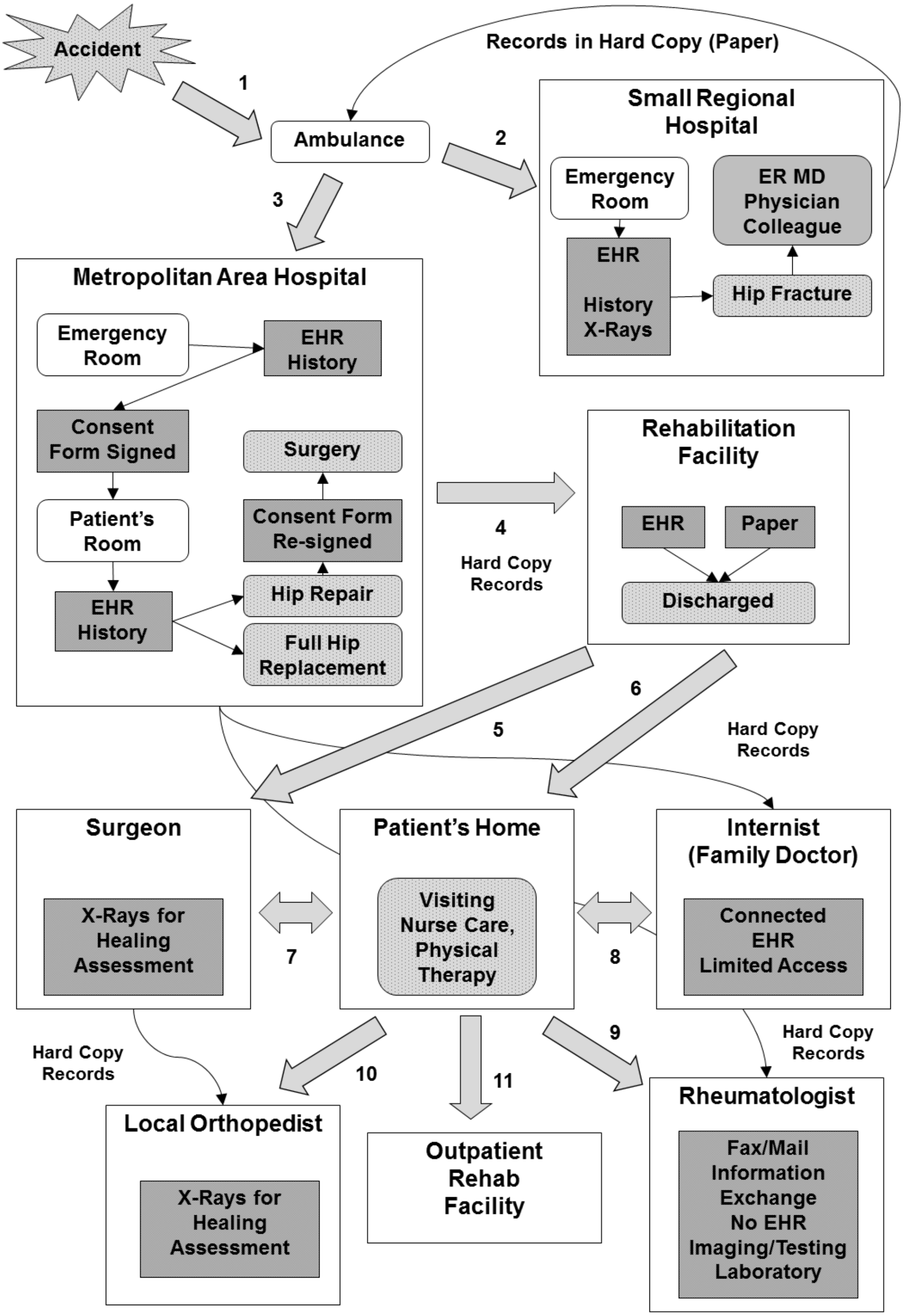
Collectively, in the United States, all of these systems target a wide range of patient care and research initiatives. First, *patient centered medical homes* can manage chronic conditions and optimize care by interacting stakeholders (e.g., family practitioner, endocrinologist, cardiologist, and nutritionist example in Section 1); in this situation, there may be a need for the lead provider to access information in other EHRs, PHRs, etc., in a timely manner in order to coordinate effective care. Second, *accountable care organizations* brings together groups of providers, clinics, hospitals, and private insurers in an effort to give coordinated care to a panel of Medicare patients in order to attempt to reduce or eliminate duplicate test and procedures for patients that visit multiple providers and have chronic conditions. Third, *secondary use* of clinical data allows providers and researchers to analyze specific diseases and their treatments across a large patient base via a clinical research data warehouse, seeking events such as adverse drug reactions, infection monitoring, or disease monitoring in a larger population (the flu epidemic in the United States in 2013). Fourth, *meaningful use* is focusing on the adoption and use of HIT within organizations that may lead to improvements in the reporting of care by offering providers incentives to acquire and deploy technology. Fifth, *personalized medicine* is targeting the treatment of an individual based on their unique medical profiles that might include specific types of diseases and focus on the use of a patient's genomic information.

In support of these aforementioned initiatives, health information exchange is vital to insure that the correct data is available at the appropriate time in a usable fashion by a specific stakeholder. In the United States, what is shared in health information exchange is most often determined by the institute that owns the data; it doesn't mean all of the data is shared. In these cases, it is common to see that the data to be shared is off-loaded into another server intended for that purpose so that there is no impact on the real-time usage of an EHR to treat patients. For example, health information exchange allows sharing so that in emergent situations providers can retrieve data on a patient from a system they are not authorized via techniques such as dynamic certification. Alternatively, health information exchange can be used to construct a clinical research data warehouse via an electronic extract, transform, and load (ETL) process from an EHR database, which in turn can provide, for example, workflows and ontologies for managing tissue data including controls for patient consent relating to tissues and boundaries on experimental uses. Health information exchange and other means of extracting clinical and claims (and other) data can also be utilized to support detailed data analysis for secondary use, accountable care organizations, and meaningful use, providing de-identified data to clinical researchers so that best practices can be evaluated across a wide range of clinical settings. This paper considers all of the above factors in order to propose an architecture in Section 4 specifically aimed for the United States health care domain that ideally achieves security across this entire spectrum of standards, regulations, HIT systems and their usage by stakeholders, coupled with health information exchange and supporting a wide range of data analyses.

3. A LACK OF SECURITY AND INFORMATION EXCHANGE IN DIGITAL HEALTH CARE

To better understand health care and the impact of HIT on patient care in the United States, this section along with Figure 1 provides a realistic case study of one co-author navigating through a complex process. Consider that a 54 year old man falls while working in the yard, and breaks his hip; an ambulance (Step 1 in Figure 1) takes him to the emergency room of a small regional hospital (Step 2) where a history is taken using an EHR at the hospital, X-rays are ordered, and a hip fracture is found. After speaking with the emergency room physician, and talking to a physician colleague, the patient decides to transfer by ambulance (Step 3) to a metropolitan area hospital, and his records are sent in hard copy. Upon arriving at the emergency room of that hospital, another patient history is taken for that hospital's EHR to capture the same information. The same story is told to the emergency room physician, orthopedic resident, etc., and at 2AM in the morning he signs a consent form for either a partial or full hip replacement. At 7AM the transport team arrives to take him to the operating room; at

Figure 1. Illustrating a sample health care process of the United States



that point, the orthopedic surgeon has another option, to repair the hip with a plate and screws, and the patient, after consulting with his physician colleague, has to re-initial the hardcopy consent form. Surgery is successful, and after three more days in the hospital, the patient is discharged to a rehab facility, (Step 4) with a hard copy of his records. The rehab center is mostly paper-based; they have an electronic system, but the medication list is hard copy as the nurse dispenses meds to patients. After 5 weeks, the patient is discharged (Step 6) to his home, and the Visiting Nurse Association in his area is assigned to monitor his care via a nurse and in home physically therapy.

During the time at rehab and at home, the patient visits the surgeon (Step 5 and Step 7) in order for X-rays to assess the healing, and also meets with his internist (Step 8) for follow up care. The internist has an electronic medical record (EMR) and can download all tests done at an external lab facility, but records at the hospital will have to be faxed and then scanned and put into the EHR as images (unsearchable). Ten weeks after the fracture, the patient is given his release from the orthopedic surgeon (Step 7) with weight bearing, and asks for that care to be managed by a local orthopedist (Step 10). The patient requests that the medical records be sent to the local orthopedist, but 2 weeks later at the appointment, no records have arrived; as a result, new and old X-rays can't be compared. Due to the unusualness of a hip fracture of a 54 year old, the patient is referred to a rheumatologist (Step 9), and brings a hard copy of some of his medical records to the appointment; blood work and a bone scan that determines that the patient has osteoporosis. The rheumatologist's office has no EHR, but can access systems at an imaging facility and testing laboratory; the rheumatologist's also makes a medical record request from hospital. Consider that even with the advance of technology and its availability, fax and snail mail are still playing a dominant role in the way that we transfer healthcare data. How can a rheumatologist without an EHR get all of the information needed from multiple sources in a timely fashion so as not to delay treatment? Clearly, even if we can deal with security for digital health care, there will still be a huge hole in the overall security of patient data with information in so many different and incompatible locations and continued dependence on paper.

Further, suppose that a clinical researcher was interested in conducting a study of males 50-60 who have hip fractures and osteoporosis, and what they may have in common (e.g., low vitamin D, low testosterone, low calcium, etc.). The dramatic push to digitize clinical data via EHRs has led to an unprecedented opportunity for clinical and public health studies (Shea et al., 2010; Wang et al., 2008; Wang et al., 2009; Jha et al., 2009). This growth is being fueled by recent federal legislation that provides generous financial incentives to institutions demonstrating aggressive application and meaningful use of comprehensive EHRs (Shea et al, 2010). Efforts are already underway to link these EHRs across institutions, and standardize the definition of phenotypes for large-scale studies of disease onset and treatment outcome, specifically within the context of routine clinical care (McCarty et al, 2010; Pace et al., 2009; Ritchie et al., 2010). The longitudinal nature of the data contained within EHRs makes them ideal for quantifying outcomes from the utilization of prescription medications (both efficacy and toxicity). More recently, huge efforts have been initiated to link new and existing EHR databases to accelerate research in personalized medicine (McCarty et al, 2010). This is a herculean task in most of the clinical environment with a heterogeneous and poorly integrated informatics infrastructure, since to find enough of a patient cohort, the researcher would need to query multiple hospitals, surgeons, laboratories, internists, and rheumatologists. At the present time in health care in the United States, health information exchange has not advanced to a stage to support such queries in any reasonable time frame. In such a scenario, how can the security issues that span multiple health information technology systems each with their own security control (with local HIPAA compliance) be brought together to securely obtain this data (with a more global HIPAA compliance) into a de-identified clinical research data warehouse to facilitate the research? How is data securely gathered into this data warehouse from paper sources? How is institutional review board approval obtained when the patients may be from multiple institutions? How is HIPAA compliance of hard-paper copies at physician offices that are transferred via fax and/or snail mail protected until they are entered into the clinical research data warehouse repository?

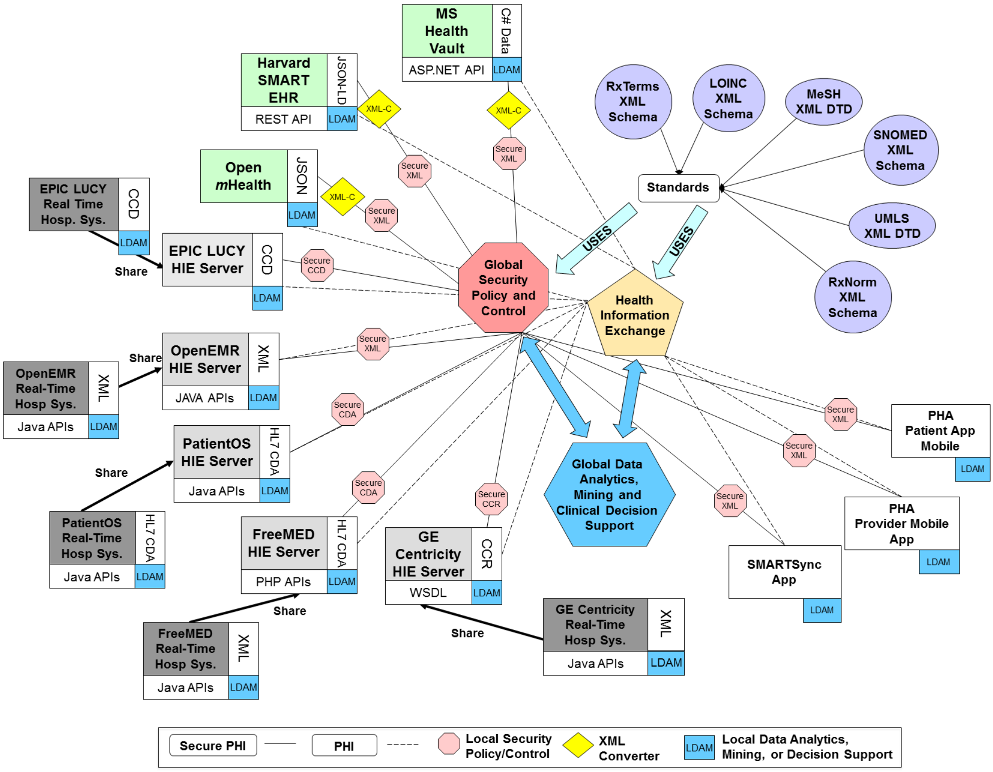
Security for digital health care in the United States must anticipate a future where the medical community has caught up with the use of HIT, and must consider EHR vendors that do not wish to allow their information to be easily shared, as do hospitals, since they deem sharing of data to cause the potential for loss of patients to other hospitals. The EHRs for the regional and metropolitan hospitals do not share data, and may not share data with local providers (e.g., internists, rheumatologists, local orthopedist, etc.). Do we define a solution with the expectation that we are planning for a futuristic scenario where secure sharing and exchange is the norm and HIT is in almost all providers? Is this even realistic in today's medical system in the United States or even within the next 5 years? 10 years?

4. PROPOSED ARCHITECTURE FOR SECURE DIGITAL HEALTH CARE

For successful health information exchange, the security of constituent systems must be integrated and support the application's need. What happens when security privileges of individual systems are in conflict with one another? How do we reconcile these local security policies? Is it possible to define a global encompassing security policy providing a level of guarantee to the local security policies from an enforcement perspective? As today's health care applications continue to become more complex and widespread, interacting with many other systems (or applications) using varied technologies, there is a need for some degree of assurance that security for the application (global) is consistent with the sum of the parts (local security) of the constituent systems.

To place our work into its perspective, Figure 2 shows our viewpoint one way that health information technology systems, medical document standards (usually achieved with extensions to XML), and end-user applications interplay with one another to provide an infrastructure for *patient centered medical homes*, *accountable care organizations*, *secondary use*, *meaningful use*, and *personalized medicine* (see Section 2 again). We examine the infrastructure from three viewpoints. The first viewpoint involves the reconciliation of security (local and global) to insure that the required clinical data reaches the providers involved in patient centered medical homes and personalized medicine where data mining and knowledge discovery techniques can be used.

Figure 2. Proposed health information exchange architecture with information security and analytics in the United States



The second viewpoint focuses on the availability of de-identified patient data for providers and clinical researchers via privacy-preserving data publishing and sharing in support of accountable care organizations, secondary use, and meaningful use, that can then in turn be used for data analysis, mining, and clinical decision support to learn what works and what doesn't in terms of treatments of various illnesses and diseases. The third viewpoint facilitates the first two viewpoints via the use of: XML and associated standards for patient and clinical data (Clinical Document Architecture, Continuity of Care Record, etc.); and, ontologies that augment this data with relevant tags that add meaning (SNOMED, LOINC, NDF-RT[20], etc.).

The lower left of Figure 2 contains examples of EHR systems (EPIC Lucy[21], OpenEMR[22], PatientOS[23], GE Centricity[24], FreeMED[25]) that share an ability to export patient data, in XML formats or standards, via the use of a proxy server in which data from the EHR has been offloaded. Emerging platforms (Open mHealth[26]to promote mobile health via an open architecture and the Harvard SMART[27] platform for substitutable medical applications that promote reuse) and personal health records (Microsoft HealthVault[28]) are presented in the upper-left of Figure 2. Open mHealth uses JSON to model patient data, while SMART uses RDF/XML and JSON-LD. In order to provide a common layer of document format, these choices of data formats must be converted (as shown by the XML-C diamond) before they can be secured and utilized.

The bottom right of Figure 2 contains examples of medical applications that must be securely managed, PHA and SMARTSync. Personal Health Assistant is an in-house developed mobile (not publicly available) test-bed application for health information management that allows: patients to view and update their personal health record stored in their Microsoft HealthVault account and authorize medical providers to access certain portion of protected health information; and, for providers to obtain the permitted information from their respective patients that they have been authorized to view. The patient version of Personal Health Assistant allows users to perform a set of actions regarding their health information. Users can view and edit their medication list, allergies, observations of daily living, and set security policies for read/write permissions on their medical providers by role as reported in our prior work (De la Rosa Algarín et al., 2013). Security settings can be set at a fine granular level, and each provider gets specific view/update authorizations to the different information components available in Personal Health Assistant. The provider version of Personal Health Assistant allows the users (health professionals) to view and edit the medical information of their patients as long as there are permitted to do so as dictated by the security set by the user (patient).

SMARTSync is an in-house developed (not publicly available) web-based test-bed medication reconciliation application used to create and preserve a patient's medication list through transfers among locations of care, preventing immediate interactions, and avoiding dosage errors in situations where brand and generic drugs are received or multi-component drugs are used. Significant risks include: overmedication when a provider prescribes a new medication (or one from the same class) or when an interacting medication is prescribed; adverse interactions, the result of conflicts between medications, which can change effect strength or serum concentration; and adverse reactions, allergic/other effects, experienced by patients which can result in a patient being wrongly labeled as allergic to a medication, unnecessarily excluding it as a treatment option in the future. To accomplish this, we gathered data form HealthVault and the SMART EHR (Ziminski et al., 2012). The upper right of Figure 2 contains the various standards for medical information, such as RxTerms and RxNorm (services to augment medication information), medical codes (SNOMED), medical nomenclature (UMLS and MeSH), and laboratory codes (LOINC), all of which are used by HIT systems and applications. In addition, local data analytics, data mining, or decision support (blue square component of systems) can be found in institutional HIT systems, patient personal health record solutions or end-point applications (e.g., SMARTSync, Personal Health Assistant). This data analytics component exists in a globalized manner; where researchers external to all of the local components will need access to information found in distributed HIT systems.

The main aspects that allow all the interaction to occur across Figure 2 are presented by the Health Information Exchange component (pentagon), which uses dotted lines to indicate the necessity to share data among HIT endpoints. The Global Security Policy and Control (octagon) component provides a centralized representation of which interactions between HIT can occur. The Global Data Analytics, Mining and Clinical Decision Support component (hexagon), which in conjunction with its local counterparts (Local Data Analytics Mining, or Decision Support, LDAM, in each respective system), provides the communication between researchers who seek data to discover hidden knowledge (on a global perspective). Note that while these components are shown in a centralized manner in Figure 2, they aim to represent an abstraction layer between all of the HIT systems. In the United States, the health informatics domain landscape is a federated architecture by nature. Thus, the end result and major challenge presented in Figure 2 is the recognition of a greater need for a comprehensive approach to security at global and local levels operating within an environment that is driven to share data through health information exchange. This comprehensive approach needs to take into consideration the distributed nature of repositories, the fragmentation of patient data across these systems, the discrepancies on sharing and security policies set in each component, as well as the potential usage of parties that do not own the data and are merely borrowing it in a predetermined set of constraints (e.g., time, amount, demographic, etc.).

At a global level, data mining techniques are useful tools in solving security related problems (Lin et al., 1996), permitting the extraction of information or knowledge from collected data or observed examples using statistical algorithms. Data mining methods have applications in intrusion detection, insider analysis, and many other settings (Lin et al., 1996; Zhu et al., 2007). Particularly, for the proposed security infrastructure (Figure 2), the reconciliation of security policies at both global and local levels may benefit from mining large-scale data transition-recording files or security monitoring of log files. The knowledge patterns detected from the mining steps may bring insights into a revision of the existing policies and a better reconciliation. For instance, cloud computing may become a necessary resource for health information exchange (Khorshed et al., 2011) allowing access to patient data by medical providers who are outside the scope (institution) of an EHR. In a cloud-computing context, insiders may be expanded from organization internal employees and contractors to cloud internal employees and contractors, cloud customers, and cloud third party suppliers. This expansion increases the exposed threats on a healthcare organization's sensitive data, such as protected health information that is being transitioned between and shared among different organizations. Data mining such as cluster analysis, novelty detection, and association rule mining can be used to examine data-access log files and detect abnormal patterns in transactions.

The practice in knowledge discovery from large compiled data also imposes great challenges to security, especially during the process of sharing EHR data. The national and state healthcare agencies in the United States routinely publish patient data from EHRs for secondary data analysis that aims to expand knowledge about disease and treatments in order to enhance healthcare experience for individuals. The access and aggregation of EHRs poses significant concerns about patient privacy and confidentiality. According to HIPAA, de-identified healthcare information may be used and disclosed for secondary analysis and represents the extraction of personal identifiers in a record so that it is difficult to re-link the data to the people mentioned in the original records. To complement this, anonymized means that all of the links between a person and the person's record have been irreversibly broken so that it would be impossible to re-identify the person in the records. However, in large-scale secondary analysis of multiple data sources that involve race, ethnicity, gender, service date, diagnosis codes (ICD-10[29]), or procedure codes, by cross linking these data sets with other publicly available databases, data mining methods may be able to associate an individual with specific diagnoses. For example, one such effort demonstrated that an individual could be re-identified by linking certain attributes in a published data set with a voter registry (Cambridge, MA (Sweeny, 2002)). The reality is that no guarantees can be given in practice.

5. RECOMMENDATIONS FOR SECURE DIGITAL HEALTH CARE

Our major assumption in this section is that a significant barrier for integrated patient care data access in the United States occurs when a stakeholder, who needs to access information from a HIT system, has not been previously authorized to use the required information (in either a routine or emergent situation) and as a result is not easily authenticated to access information from systems that they have not been previously authorized to the individual. We recognize that in order to provide proper security, any recommendations must cover the storage and transmission of protected health information and personally identifiable information data. In this section, we provide our viewpoint of the a set of recommendations across a broad range of system techniques and mechanisms, as well as approaches that require human intervention in the general workflow to monitor and control secure information access. These techniques and mechanisms are readily available for use, and have been extensively deployed in other domains unlike health care. We provide our viewpoint with these recommendations in order to present the case that to provide a proper level of secure digital health care in the United States it will be necessary to leverage existing computational concepts and techniques some of which must be extended and modified for use in the health care domain.

Meta Standard for Health Care: The ability to achieve health information exchange among the myriad variety of HIT is being dramatically hindered by a lack of agreement on one standard coupled with companies that are focused on vendor specific approaches and proprietary formats that inherently limit the ability to share data. The HIT vendor community must adopt practices in their development and deployment technologies that are well accepted in other fields through agreements on standards that allow data to seamlessly flow among different systems. What approaches have been historically utilized in computing to facilitate exchange?

Consider the database field based on the SQL ANSI Standard in 1986 and an ISO standard in 1987. Today, it is trivial to exchange information in database systems (MySQL, SQL Server, Oracle, etc.) with the ability to export an entire database schema (XML) and the entire database repository into XMI instances, at which point the database in that format can be moved from one database platform to another. In programming languages, Java, introduced by Sun in 1995, changed the computing landscape with the write-once run anywhere paradigm, revolutionizing the cross platform development and dramatically improving Internet browser capabilities beyond simple HTML. Java is now dominant in the computing field across all domains and disciplines; it has simply changed the way programming was conceptualized.

These aforementioned examples in computing are the approaches that HIT vendors must adopt – they must be focused on providing a means to export their data from an EHR into a format that can be read and imported by another EHR or an external HIT system. To accomplish this, there needs to be two dramatic changes. First, the definition of a meta-standard that unifies across all of the different existing standards to provide the one single format (schema and structure) that every HIT vendor can import and/or export. Second, the need for a culture change that breaks the boundaries that are in place in regards to hospitals that sharing data will mean losing patients and for vendors that want to lock in hospitals and other medical organizations to solutions that once chosen become extremely difficult or nearly impossible to change. As easy as it is to take a database from Oracle to SQL Server to MySQL, it should be just as trivial to take a patient database from GE Centricity to Allscripts to Epic. The boundaries need to be taken down, and the true owner of the data, the patient, needs to be the one to dictate the way that their health care data is represented, shared, and exchanged; patients are being held hostage in the inability of the health care industry to effectively disseminate data.

The idea of a meta-standard for medical standards is to provide one universal and collective model that allows all types of medical data to be captured in both structure and semantics. Once established, this meta-standard can be the means for one HIT vendor to export data from its product that can then be easily loaded into another product of a different HIT vendor. Instead of focusing on health information exchange on a very low-level basis that considers linking three or four hospitals in a region, we must transcend to an approach that provides a meta-standard that raises the conceptual and abstraction level of information exchange to a place that will seamlessly allow medical providers to share information, change technologies, and adopt new technologies, without facing the overhead of custom integrations among different products. The HIE process must be simplified for effective information sharing that facilitates patient care and is not held hostage to an outmoded business model with vendor proprietary forms that limits sharing or requires custom interfaces between every interacting system.

Encryption: The distributed nature of data storage in healthcare makes it necessary to provide security at storage point, as well as in the point of transmission. An encryption framework must provide a robust level of security for stored information capable of integrating heterogeneous local solutions, in the respective data sources, in a global context. This encryption framework should be extensible to handle new types of data unique to health care (genomic, phenotypic). For secure online data transmission, existing technologies (e.g., HTTPS, SSL, etc.) should be leveraged in order to provide a proper level of protection. The HITECH Act achieves protected health information portability and storage through encryption as applied to hard drives and (portable) systems such as laptops, jump drives, desktops, smart phones, tablets, cloud inter-system links, and user-system links (Mavridis et al., 2001).

Certificates: X.509 certificates and their ability to be extended via certificate attributes can allow, over time, a user to acquire multiple X.509 certificates (each to access a specific system) based on their activity being authorized to utilize different systems. The advantage of multiple certificates (one per work setting) is to minimize the impact for failure; with a single certificate and multiple attribute certificates (one for each work setting) failure may compromise multiple settings, while multiple certificates (one per work setting) should limit the impact of failure. Each work setting can have their own security infrastructure and algorithms to generate a public-private key; the concept of multiple certificates each with multiple attribute certificates attached is akin to a wallet with multiple cards issued from different sources (Mavridis et al., 2001). Related efforts include: a framework for secure e-Health authentication using a multiple factor approach where physicians would provide multiple pieces of information in emergent situations akin to our multiple certificate approach (Boonyarattaphan et al., 2009); and, a framework for adaptive trust negotiation that establishes trust based on attributes other than identity (Ryutov et al., 2005).

DIRECT and Health Information Service Provider: DIRECT[30] allows individuals, providers and organizations to share information with best practices that have trust and privacy considerations that are very consistent to the privacy emphasis of this proposal. A Health Information Service Provider is used to describe the management of security and transport for directed exchange and an organizational model that performs health information service provider functions to allow interactions of HIPAA Covered Entities with the sender or receiver of directed exchange of personally identifiable information, and must include all data collection, use, retention, and disclosure policies. In practice, sender and receiver take sole responsibility for encryption/decryption activities through the use of standardized encryption algorithms. In Figure 2, there would be service providers for each of the data sources (EHRs and personal health records). Health information service providers could use X.509 certificates as previously defined, where a certificate by role could be established for the different role each stakeholder coupd play. Attribute certificates can be associated with various characteristics such as for the data level (HIPPA, FERPA, DE-IDs), the situation (Urgent care, Primary Care, Inpatient Care), the type of data (patient, genomic, de-identified), etc. In an emergent situation where a physician might need access to another EHR, s/he could present her/his X.509 certificates and a process can be initiated by the user to consult among the EHRs with two possible results: access is allowed to the physician based on submitted certificates (with some expiration) or not.

Access Control: Access control models provide the benefit of applying security at different levels of the information exchange scenario. Given the structure of Figure 2, role-based access control (Sandhu et al., 2000) could be used as a cornerstone, but needs extensions for health care. Extension parameters include patient, healthcare facility, task, temporal information, and other stakeholders (Berhe et al., 2010; Caine et al., 2013). Another extension would be the ability to extract local security policies and integrate them into a global one that is enforceable across the health care enterprise (Bhatti et al., 2005; De la Rosa Algarín, 2012; De la Rosa Algarín, 2013). A third extension could be for delegation of authority to facilitate access in an health information exchange setting (Berhe et al., 2010), where a provider often passes on his/her permissions (e.g., patients) to other providers. A fourth extension is the need for secure health information exchange across a wide range of data (e.g., clinical, genomic, and phenotypic) that will involve the co-consideration of HIPAA, GINA, and ELSI, and the exploration of role based access control (RBAC) (Sandhu et al., 2000) and delegation for genomic and phenotypic data.

User-Based Security Mechanisms: There are many security nets in health care in terms of data access that happen after the misuse event has occurred. A clinician role in a hospital would have specific permissions, and an actual user should be further restricted to his/her patients. In practice, clinicians may be able to access more data than they are authorized and monitored in each single system against suspicious patient data retrieval (Barrows et al., 1996), and this is done after the fact via an audit. However, as given in Figure 2, the detection of intruders or system misuse is going to be necessary and will require more sophisticated network monitoring tools against consolidated log files from all of the constituent HIT systems that are interoperating. One dominant approach for data access for health information exchange or clinical research data warehouses is the use of an honest broker, an actual individual who is in charge of triggering the clinical (research) data request event to the corresponding HIT system(s) and returning the results to the clinical (researcher) (Silvey et al., 2008). Large hospitals require a dedicated team of patient privacy security officers in charge of enforcing regular password updates, system updates, correct system configuration, hard drive encryption, and other security related tasks; clearly this is more complex in an environment as shown in Figure 2. Often, improving user access means that clinicians must be educated on privacy regulations, procedures, system usage, and configuration, in order to avoid misconfigurations, such as using the same password for the private key, operating system login, and EHR system login that can merely achieved during dedicated seminars (Buckovich et al., 1999).

Cloud Computing: With the emergence of mobile computing, the ability to support mobile access to health care information can be leveraged via cloud computing. The benefit of moving towards cloud-based solutions includes the decreased operational cost of maintaining systems that would otherwise be found in private practices or clinics, their maintenance, and their availability (Wu et al., 2012). The magnitude of this push is evidenced by the 21% growth of the market[31], and the estimated $5.4 billion investment by the year 2017[32]. The computational benefits of moving towards cloud computing in health care are immense and include: continuous patient data monitoring, smart emergency management, always-connected mobile devices, pervasive access to patient data (new or old), etc. (Dinh et al., 2011). Security must be attained at end-user, processing, and storage layers of an application, and one approach (Zhou et al., 2010) evaluates the security concerns that cloud computing can provide to health care via availability, confidentiality, data integrity, control and audit. For example, as evidenced in (Rodrigues et al., 2013), the security risks not only involved the role-based access control for the end users (e.g. Physicians, Nurses, Administrative Personnel, Patients, etc.), but also the role-based and encryption at the third-party cloud service provider. In support for access control, the work of (Wu et al., 2012) proposes an approach that provides this level of security in selective sharing of EHRs. By aggregating the EHRs from different providers in cloud-based solutions (e.g., OpenEMR, Microsoft HealhtVault, and other shown in Figure 2) and utilizing a modular security policy manager (called the Composite EHR Access broker), role-based enforced information is disseminated. In an attempt to tackle a broader picture of cloud security in healthcare, the work of (Neame, 2013) presents a schema to tackle three main obstacles in EHR sharing: accessibility, privacy, and information functionality assurance. For privacy, the disassociation of the context (names, clinics, etc.) from the content is a simple step to follow that will result in meaningless data when not found in the appropriate respective context. For access control, an augmented security process would be needed and could include smart cards or other unique components that will assure access only from the proper identities. Lastly, in the work of (Alabdulatif et al., 2013), access control to EHRs is improved by restricting the access leveraging encrypted parameters for each user of a cloud data source.

6. CONCLUSION

This paper has looked backwards to the first discussions of privacy and access control for medical settings (Biskup, 1990; Ting, 1990), and more importantly forward to the wide array of emerging HIT systems, applications, and standards, intended to support health information exchange in order to allow varied stakeholders to securely access information in routine and emergent situations. As a result, by focusing in the current state of affairs in health care of the United States, we conclude that security cannot be considered simply from these individual systems, but must take a approach that requires a more global security solution to protect the vast amount of data available for use by medical professionals and data analysis by researchers. Toward this objective, Section 2 presented the changing landscape of medical care, standards, and technologies, that are difficult to support without health information exchange, and is further complicated by the present state (or lack) of medical information exchange in the United States, as illustrated by a scenario of patient care recently experienced by one of the co-authors and detailed in Section 3. Based on this information, in Section 4 and Figure 2, we presented our viewpoint of an architecture that positioned the HIT systems, standards, and applications in the context of health information exchange in the United States, and introducing globalized security enforcement and data mining/analysis components. While these globalized components are shown as internal components of the overall architecture, they aim to represent an abstraction layer that must be considered from the perspective of each constituent system of the health information exchange process. Using this as a basis, the recommendation list in Section 5 is our viewpoint for a first step for a roadmap for considering the security for digital health care that transcends individual systems and must consider the diverse HIT systems, applications, standards, and their interactions currently existing and happening in the

United States; using, extending and leveraging traditional security mechanisms (encryption, access control, auditing, etc.) and user based techniques with privacy officers to control access to information via honest brokers and access via emerging platforms (mobile and cloud computing).

It is important to note that in this paper, while we have focused on the landscape on health information technology and information exchange in the United States, initiatives taken by other countries in their domestic health care systems can serve as guides for not only localized health care information technology development, but also for a broader information exchange scenario. Thus, the work presented in this paper also has an impact on EHRs, health information technology, and health information exchange in other countries. One effort of particular note is the US Department of Veterans Affairs' VistA system, which has been deployed in veteran hospitals, outpatient clinics, and nursing homes. VistA is an open source, Java-based EHR that is revolutionary in its adoption across such a wide scope, with linkages to the Department of Defense EHR to allow patients that move between the Department of Defense itself and the Veterans Affairs department with the purpose of having a complete medical history. VistA has expanded to an international setting with the creation of the WorldVistA[33] organization that has exploited VistA outside of the US with extensions for pediatrics, obstetrics, and other areas that are not supported for veterans. As another example, consider the case of the United Kingdom and its National Health Service (NHS) that covers all of the residents (Thomson et al., 2012) with several associated laws that provide: guidelines and enforcement of patient information disclosure (e.g., the Computer Misuse Act 1990[34], Access to Health Records Act 1990[35], The Data Protection Act 1998[36], and others); and, computational standards for information security (e.g., ISO/IEC 27002[37]). In addition, the NHS employs an approach towards a centralized database of patient information with NHS Spine (i.e., a centralized storage of patient data vs. the distributed local EHRs and PHRs in the United States) that has created the NHS Confidentiality campaign (a pro-confidentiality movement aimed at preserving patient information privacy). As another example, consider the Australian health care system that is universal like NHS and covers all residents and temporary-visa holding residents from countries with special relations with Australia (Thomson et al., 2012). The HIT approach of Australia has been focused on a patient-controlled EHR, much like a personal health record found in the United States. The best example is The Personally Controlled eHealth Record System[38], which provides the patient full control over their health information, specifically, what information is part of the health record itself and who can actually access the information[39]. The interested reader is referred to (Thomson et al., 2012) for a comprehensive discussion of health care systems in Australia, Canada, Denmark, England, France, Germany, Iceland, Italy, Japan, Netherlands, New Zealand, Norway, Sweden, Switzerland, and the United States.

REFERENCES

Alabdulatif, A., Khalil, I., & Mai, V. (2013). Protection of electronic health records (EHRs) in cloud. *Engineering in Medicine and Biology Society (EMBC), 2013 35th Annual International Conference of the IEEE* (pp. 4191-4194)

Barrows, R. C., & Clayton, P. D. (1996). Privacy, confidentiality, and electronic medical records. *Journal of the American Medical Informatics Association*, *3*(2), 139–148. doi:10.1136/jamia.1996.96236282 PMID:8653450

Berhe, S., Demurjian, S., Saripalle, R., Agresta, T., Liu, J., & Cusano, A. et al. Secure, Obligated and Coordinated Collaboration in Health Care for the Patient-Centered Medical Home. In: *AMIA Annual Symposium Proceedings*. Volume 2010., American Medical Informatics Association (2010) 36

Bhatti, R., Ghafoor, A., Bertino, E., & Joshi, J. B. D. (2005). X-GTRBAC: An XML-based policy specification framework and architecture for enterprise-wide access control. [TISSEC]. *ACM Transactions on Information and System Security*, *8*(2), 187–227. doi:10.1145/1065545.1065547

Biskup, J. (1990). *Protection of privacy and confidentiality in medical information systems: Problems and guidelines*. North-Holland.

Boonyarattaphan, A., Bai, Y., & Chung, S. A security framework for e-Health service authentication and e-Health data transmission. In: Communications and Information Technology, 2009. ISCIT 2009. 9th International Symposium on, IEEE (2009) 1213–1218 doi:10.1109/ISCIT.2009.5341116

Buckovich, S. A., Rippen, H. E., & Rozen, M. J. (1999). Driving Toward Guiding Principles: A Goal for Privacy, Confidentiality, and Security of Health Information. *Journal of the American Medical Informatics Association*, *6*(2), 122–133. doi:10.1136/jamia.1999.0060122 PMID:10094065

Caine, K., & Hanania, R. (2013). Patients want granular privacy control over health information in electronic medical records. *Journal of the American Medical Informatics Association*, *20*(1), 7–15. doi:10.1136/amiajnl-2012-001023 PMID:23184192

De la Rosa Algarín, A., Demurjian, S. A., Berhe, S., & Pavlich-Mariscal, J. (2012). A Security Framework for XML Schemas and Documents for Health Care. *International Workshop on Biomedical and Health Informatics*, (pp. 782–789).

De la Rosa Algarín, A., Ziminski, T. B., Demurjian, S. A., Kuykendall, R., & Rivera Sánchez, Y. (2013). Defining and Enforcing XACML Role-Based Security Policies within an XML Security Framework. *Proceedings of 9th International Conference on Web Information Systems and Technologies, INSTICC*, (pp. 16-25).

Dinh, H. T., Lee, C., Niyato, D., & Wang, P. (2011). *A survey of mobile cloud computing: architecture, applications, and approaches*. Wireless Communications and Mobile Computing.

Jha, A. K., DesRoches, C. M., Campbell, E. G., Donelan, K., Rao, S. R., & Ferris, T. G. et al. (2009). Use of electronic health records in US hospitals. *The New England Journal of Medicine*, *360*(16), 1628–1638. doi:10.1056/NEJMsa0900592 PMID:19321858

Khorshed, M. T., Ali, A. S., & Wasimi, S. A. (2011). Monitoring insider's activities in cloud computing using rule based learning. *2011 IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, (pp. 757–764).

Kwon, J., & Johnson, M. E. (2012). Security practices and regulatory compliance in the healthcare industry. *Journal of the American Medical Informatics Association*. PMID:22955497

Lin, T. Y., Hinke, T. H., Marks, D. G., & Thuraisingham, B. (1996). Security and data mining. *Database Security*, *9*, 391–399.

Mavridis, I., Georgiadis, C., Pangalos, G., & Khair, M. (2001). Access control based on attribute certificates for medical intranet applications. *Journal of Medical Internet Research*, *3*(1), e9. doi:10.2196/jmir.3.1.e9 PMID:11720951

McCarty, C. A., & Wilke, R. A. (2010). Biobanking and pharmacogenomics. *Pharmacogenomics*, *11*(5), 637–641. doi:10.2217/pgs.10.13 PMID:20415552

Neame, R. (2013). Effective Sharing of Health Records, Maintaining Privacy: A Practical Schema. *Online Journal of Public Health Informatics*, *5*(2), 217. doi:10.5210/ojphi.v5i2.4344 PMID:23923101

Pace, W. D., Cifuentes, M., Valuck, R. J., Staton, E. W., Brandt, E. C., & West, D. R. et al. (2009). An electronic practice-based network for observational comparative effectiveness research. *Annals of Internal Medicine*, *151*(5), 338. doi:10.7326/0003-4819-151-5-200909010-00140 PMID:19638402

Ritchie, M. D., Denny, J. C., Crawford, D. C., Ramirez, A. H., Weiner, J. B., & Pulley, J. M. et al. (2010). Robust replication of genotype-phenotype associations across multiple diseases in an electronic medical record. *American Journal of Human Genetics*, *86*(4), 560–572. doi:10.1016/j.ajhg.2010.03.003 PMID:20362271

Rodrigues, J. J., de la Torre, I., Fernández, G., & López-Coronado, M. (2013). Analysis of the Security and Privacy Requirements of Cloud-Based Electronic Health Records Systems. *Journal of Medical Internet Research*, *15*(8). PMID:23965254

Ryutov, T., Zhou, L., Neuman, C., Leithead, T., & Seamons, K. E. (2005). Adaptive trust negotiation and access control. *Proceedings of the tenth ACM symposium on Access control models and technologies*, ACM, (pp. 139–146). doi:10.1145/1063979.1064004

Sandhu, R., Ferraiolo, D., & Kuhn, R. (2000). The NIST model for role-based access control: towards a unified standard. *Symposium on Access Control Models and Technologies: Proceedings of the fifth ACM workshop on Role-based access control*, (26), (pp. 47–63). doi:10.1145/344287.344301

Shea, S., & Hripcsak, G. (2010). Accelerating the use of electronic health records in physician practices. *The New England Journal of Medicine*, *362*(3), 192–195. doi:10.1056/NEJMp0910140 PMID:20089969

Silvey, S. A., Schulte, J., Smaltz, D. H., & Kamal, J. et al. (2008). Honest broker protocol streamlines research access to data while safeguarding patient privacy. *Annual Symposium proceedings/AMIA Symposium*, (pp. 1133).

Sweeney, L. (2002). k-anonymity: A model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-based Systems*, *10*(05), 557–570. doi:10.1142/S0218488502001648

Thomson, S., Osborn, R., Squires, D., & Jun, M. (2012). *International profiles of health care systems, 2012*. New York: The Commonwealth Fund.

Ting, TC. (199). *Application information security semantics: A case of mental health delivery*.

Wang, X., Chused, A., Elhadad, N., Friedman, C., & Markatou, M. (2008). Automated knowledge acquisition from clinical narrative reports. *AMIA Annual Symposium Proceedings*, (pp. 783).

Wang, X., Hripcsak, G., Markatou, M., & Friedman, C. (2009). Active computerized pharmacovigilance using natural language processing, statistics, and electronic health records: A feasibility study. *Journal of the American Medical Informatics Association*, *16*(3), 328–337. doi:10.1197/jamia.M3028 PMID:19261932

Wu, R., Ahn, G. J., & Hu, H. (2012). Secure sharing of electronic health records in clouds. *2012 8th International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom)*, (pp. 711-718)

Zhou, M., Zhang, R., Xie, W., Qian, W., & Zhou, A. (2010). Security and privacy in cloud computing: A survey. *2010 Sixth International Conference on Semantics Knowledge and Grid (SKG)*, (pp. 105-112) doi:10.1109/SKG.2010.19

Zhu, D., Premkumar, G., Zhang, X., & Chu, C. H. (2007). Data Mining for Network Intrusion Detection: A Comparison of Alternative Methods*. *Decision Sciences*, *32*(4), 635–660. doi:10.1111/j.1540-5915.2001.tb00975.x

Ziminski, T. B., De la Rosa Algarín, A., Saripalle, R., Demurjian, S. A., & Jackson, E. (2012). SMART-Sync: Towards Patient-Driven Medication Reconciliation Using the SMART Framework. *International Workshop on Biomedical and Health Informatics*, (pp. 806–813).

ENDNOTES

[1] http://www.hhs.gov/ocr/privacy/

[2] http://www.genome.gov/24519851

[3] http://www.aafp.org/online/en/home/publications/news/news-now/practice-professional-issues/20130201ehradoptrates.html

[4] http://www.informationweek.com/healthcare/electronic-medical-records/ehr-adoption-us-remains-the-slow-poke/240142152

[5] http://pcmh.ahrq.gov/

[6] http://www.innovations.cms.gov/initiatives/ACO/index.html

[7] http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Meaningful_Use.html

[8] http://www.hl7.org/implement/standards/product_brief.cfm?product_id=7

[9] http://www.astm.org/Standards/E2369.htm

[10] http://loinc.org/

[11] http://www.ihtsdo.org/snomed-ct/

[12] http://www.nlm.nih.gov/research/umls/

[13] http://www.w3.org/XML/

[14] http://www.w3.org/RDF/

[15] http://www.json.org/

[16] http://www.allscripts.com/

[17] http://www3.gehealthcare.com/en/Products/Categories/Healthcare_IT

[18] http://www.ehealth.va.gov/VistA.asp

[19] http://www.genomas.net/

[20] http://www.nlm.nih.gov/research/umls/sourcereleasedocs/current/NDFRT/

[21] http://www.epic.com/software-phr.php

[22] http://www.open-emr.org/

[23] http://www.patientos.org/

[24] http://www3.gehealthcare.com/en/Products/Categories/Healthcare_IT/Electronic_Medical_Records/Centricity_EMR

[25] http://freemedsoftware.org/

[26] http://openmhealth.org/

[27] http://smartplatforms.org/

[28] https://www.healthvault.com

[29] http://apps.who.int/classifications/icd10/browse/2010/en

[30] http://wiki.directproject.org/

[31] http://www.prweb.com/releases/2013/9/prweb11146871.htm

[32] http://cloudtimes.org/2013/09/30/the-health-care-sector-will-invest-5-4-billion-in-cloud-computing-by-2017/

[33] http://worldvista.org/

[34] http://www.legislation.gov.uk/ukpga/1990/18/contents

[35] http://www.legislation.gov.uk/ukpga/1990/23/contents

[36] http://www.legislation.gov.uk/ukpga/1998/29/contents

[37] http://webstore.iec.ch/preview/info_isoiec27002%7Bed1.0%7Den.pdf

[38] http://www.ehealth.gov.au

[39] http://www.ehealth.gov.au/internet/ehealth/publishing.nsf/Content/ehealth_privacy