SAIS 2013Proceedings

Southern (SAIS)

5-18-2013

THE UNIQUE PATIENT IDENTIFICATION (UPI) DEBATE: IMPLEMENTING A U.S. PATIENT IDENTIFICATION STANDARD

Don Montgomery
Southern Polytechnic State University, me@donmontgomery.com

Chi Zhang
Southern Polytechnic State University, chizhang@spsu.edu

THE UNIQUE PATIENT IDENTIFICATION (UPI) DEBATE: IMPLEMENTING A U.S. PATIENT IDENTIFICATION STANDARD

Don Montgomery
Southern Polytechnic State University
me@donmontgomery.com

Chi Zhang
Southern Polytechnic State University
chizhang@spsu.edu

ABSTRACT

This study provides a comparison and contrast of the merits surrounding the implementation of a US national unique patient identification (UPI) system. Based on the lack of trust created in the minds of current US patients in how current medical records are distributed throughout the US medical system, this study reviews the UPI initiative in India, public trust concerns in the United Kingdom (UK), and trials and feedback from research and clinical review by the US medical community concerning the pros and cons of such a system. This study leads to a proposed patient trusted solution that could be implemented for the purpose of tracking and protecting confidential patient information in the US via the latest cloud based technologies. The proposed solution intends to bring more patient trust to the entire US national medical information technology system as a whole.

Keywords

Health Information Exchanges (HIE), Unique Patient Identification (UPI), Electronic Health Records (EHR)

INTRODUCTION

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) passed by Congress required a unique health identifier to be issued for each individual, employer, health plan and health care provider for use in the health care system, but Congress was forced in 1998 to prohibit funding for the unique patient identifier (UPI) due to the public outcry for privacy and security concerns. New federal regulations under the Patient Protection and Affordable Care Act (PPACA) may now be attempting to end the 1998 prohibition (Brase, 2012).

A UPI is a “unique, non-disclosing (i.e., containing no personal information) patient identifier” to “accurately link, file, and retrieve individual health records” (Hillestand, Bigelow, Chaudhry, Dreyer, & Greenberg, et. al, 2008). It provides a uniform way to easily and correctly identify patients, link the patients to their health data and allow broad sharing, monitoring, research and analysis (Brase, 2012). The benefits of developing electronic health records and a UPI are believed to result in improved quality of medical care and reduced administrative costs.

This study provides a comparison and contrast of the merits surrounding the implementation of a US national unique patient identification (UPI) system. Based on the lack of trust created in the minds of current US patients in how current medical records are distributed throughout the US medical system, this study reviews a national UPI initiative in the nation of India, public trust concerns in the United Kingdom (UK), and research trials and feedback from research and clinical review by the US academic community concerning the pros and cons of such a system. Several nations worldwide have proposed or have attempted to implement a national unique patient identification (UPI) system to act as a “primary key” for all records and integrated systems. (Saenz, 2010, September 13). In the debate of adopting a national UPI system for the United States, this study tries to review and answer the following questions:

1. What are the pros and cons of implementing a national UPI system?
2. What obstacles and failures have occurred in another country’s implementation?
3. How does patient trust factor into the public’s interest in a national UPI system?
4. Is there a way to get the benefits of a national UPI without creating a new US federal infrastructure or department?

This study attempts to make the case that patient trust in the technological solution is a major factor in the success of this type of system, and the advance of new cloud computing and mobile technologies may bring forth a new opportunity to offer a successful UPI model in the US.

LITERATURE REVIEW

What are the pros and cons of implementing a national UPI system?

The debate over a US national UPI standard presents two clear opposing views on the issue - access vs. privacy (Greenberg & Ridgely, 2008; Collins & Peel, 2012). The affirmative position is that a national UPI for all patients in the system will decrease poor information accuracy substantially. Those opposed make the case that a national UPI will create patient privacy issues.

The U.S. health care system is composed of numerous independent systems, each with their own method of identifying patients, which makes linking patients across systems very difficult. Currently a "statistical matching" criteria is used based on multiple personal attributes (e.g., name, address, birth date, medical-record numbers and all or part of social security number) as a primary approach to this linking. This approach has been shown by published data to have a high rate of errors of duplicate or split records (Hillestand, Bigelow, Chaudhry, Dreyer, & Greenberg, et. al, 2008). The proponents of a national UPI in the US make the point that linking wrong or errant records to patients is inherently dangerous to the safety of the patients. (American College of Cardiology Health IT Committee, n.d.) The result leaves open the possibility that a physician may have "incomplete information when treating a patient" (American College of Cardiology Health IT Committee, n.d.).

The main concession the detractors are requesting from the proponents of a national UPI system is that the system must require the written consent of the patient before information can be disseminated (American College of Cardiology Health IT Committee, n.d.). Proponents scoff at this request noting that a physician needs all of the patient information available to make a proper diagnosis (AHIMA, 2009). Also, the written consent requirement does not take into account the possibility that that patient may be incapacitated at the time the UPI data is needed (American College of Cardiology Health IT Committee, n.d.). The desire for total information access by UPI proponents of patient information seems to preclude patient privacy concerns and could force the design of a technological solution that is devoid of patient privacy control mechanisms. That is exactly what occurred in the design of India's patient ID system discussed later in this study. Can technology accommodate both requirements?

The US Congress has shelved the use of a national UPI since 1999 (Hillestand, Bigelow, Chaudhry, Dreyer, & Greenberg, et. al, 2008). Proponents of a national UPI initiative are readdressing the issue again this year with Congress; however, the proposal's focus is strictly focused on technology and not gaining patient trust in the proposed system (Terry, 2012, September, 26). This is the same failed approach when Congress did not provide a pharmaceutical prescription drug tracking system, yet provided tracking for healthcare apparatus technology (Palmer, 2012, July 5). This study attempts to provide new research information that may be helpful for reconsidering this issue.

What obstacles and failures have occurred in another country's national UPI implementation?

To answer this question and to learn from the experience of prior efforts in implementing a national UPI system, the most recent national UPI initiative in the country of India is reviewed here. India recently attempted to implement a national UPI system without trust design factors and the results were negative. In 2010, the country of India launched a full scale national patient identification system. They attempted to create a single government medical database by gather the biometric information of over 1.2 billion people in their country for the sole purpose of creating a national unique identification number (UID) (Kakkar, 2011, December 14). The Unique Identification Authority of India planned on paying for this program by selling licensing fees to commercial entities that could use the information to verify customers, and vendor's staff (Kakkar, 2011, December 14).

Any resident of India could apply for and receive a UID. That meant that non-citizens could use the UID to garner services that may have not been previously permitted prior to the UID system. Despite the many advantages that unique identification offers from a technology perspective, the majority of citizens lack the trust in the system needed for it to be widely adapted. (Kakkar, 2011, December 14).

Critics of the plan were disturbed by the potential use of the system to locate and isolate specific groups and individuals. The extreme detractors even warned of the system's use for genocide (Saenz, 2010, September 13). After two years, the out pouring of distrust from a majority of the citizenry and a lack of solid political support from the Indian government, led to the rejection of the UIDIA being formed (Saenz, 2010, September 13).

India's implementation of a UID standard provides a unique case study in the ramifications of information technology solutions design that is devoid of patient trust in its implementation. The obvious result is a complete failure of the patient community to embrace the solution. User trust across all participants is the defining factor in designing a feasible UPI system in the US. Examining trust, and how it relates to a UPI system design, requires further investigation.

How does patient trust factor into the public's interest in a national UPI system?

Before technology can be designed and implemented, acceptance of the reasoning behind the technological solution must be agreed to and accepted in the minds of the American patients. Patient trust is the key factor to creating a successful UPI implementation. This research has reviewed a specific large scale implementation that lacked patient trust during the design phase that ended in failure for the entire effort.

It seems that the Internet has provided the patient community with "another opinion" (Parker-Pope, 2006, July 25). Parker-Pope's (2006, July 25) research infers that perceived trust between doctors and patients are negatively affected when the patient's self-directed research conflicts with a doctor's treatment recommendation. Many doctors sense the distrust in patients that come into their clinic with a pre-conceived diagnosis, and get irritated when the doctor does not prescribe what the patient believes the treatment should be (Parker-Pope, 2006, July 25).

However, when the doctor presents information via information technology channels to a patient prior to the patient's own research, a more positive trust outcome occurs. A recent study conducted by Richard Klein (2007) at Clemson University focused on the use of Internet technologies to act as a communication channel between patients and physicians after on-site visits. The findings were surprising. The research validated a "core component of the vast majority (of the) technology acceptance theory, namely behavioral intentions translate into use behaviors" (Klein, 2007). Therefore, patient perception of usefulness can influence ultimate acceptance (Klein, 2007).

The research suggests that the more the patient perceives technology as a useful tool for gathering comprehendible medical information, the more they will use it and trust its findings – even over the professional opinion of the patient's personal physician. However, if the physician and the patient work together at the initial treatment research phase, trust created through patient information empowerment may encourage patient participation in offering information back into the system as well (Rynning, 2007). This has been confirmed in a recent UC Davis and the University of Southern California patient-doctor trust study. (Hu, Bell, Kravitz, & Orrange, 2012). The UC Davis study found that doctors encouraging Internet research allowed the patients to feel more in "control" of their treatment. Control of the shared treatment information or care is the key to trust in this study. (Hu, Bell, Kravitz, & Orrange, 2012).

The failure of the India UID system seems to correlate with Klein's findings. The designers of the UID obviously failed at getting a sufficient amount of the patient community to abide the benefits of such a system before implementation. Even though there was grave patient opposition, the UID system designers proceeded nonetheless. Lack of patient trust was the fatal flaw in the design. How do we define trust in the design process?

Patients and the Design Process

Was it necessary for patients to actually be a part of the design process? Some might make the logical conclusion that the patients or users of the system must have a say in any UPI's design implementation in order to get a feeling of trust in the system. Rowe's European Journal of Public Health published research on physician-patient trust (February 2006) found that patient participation per se does not necessarily result in higher trust. Instead, a clinician's technical competence, respect for patient views, information sharing, and their confidence in the patient's ability to manage their illness played major factors in trust (Rowe & Calnan, 2006, February, p. 5).

This research suggests that if patients see the advantages of a UPI system, and can expect very low or no adverse results in participating, then participation should be expected, despite being a non-participant in the solution's design. Rynning (2007) continues by stating that "certain risks of privacy infringements can be reduced by the introduction of sufficiently refined and effective systems for access and authorization, control, encryption, or even anonymization of certain data and the use of other privacy enhancing technologies." It is this reasoning that leads this study to conclude the need for a market based information exchange network that will be discussed later.

Rynnings research is based on Physician to Patient trust factors, but can this be extended to organizations and governments? Unfortunately, little research has been done on patient's institutional trust levels. It was this lack of research that may have led to the failure of the India UID implementation.

UPI Trust in Decline in Other Countries

Empirical evidence suggests in countries like the UK, public trust in UPI security is believed to be in decline (Rowe & Calnan, 2006, February). The political response is to seek performance management as a mechanism for rebuilding public trust (Rowe & Calnan, 2006, February). "Rather than relying on traditional processes of professional self-regulation to ensure high standards of competence and conduct, governments are increasingly turning to external agencies to regulate, monitor, and publicly report on the quality of care" (Rowe & Calnan, 2006, February). A successful UPI design requires third-party UPI monitoring. The UK government agency, NHS, lost 1.8 million records in the UK in 2012 or 5000 records per day (Doyle, 2012, October 28). In the UK, the hospitals monitor the records, clearly this approach is flawed, and this study proposes a more effective solution. The research discussed here shows that the distrust is based on perceived restriction and centralized control of patient information and treatment solutions by the medical community, not the availability of information itself. If the factors of patient trust in information technology information can be defined, it could be possible to implement access control factors into the design of a US national UPI system acceptable to the patient community and health community at large in the US.

Defining the Factors of Patient Trust

It is clear that institutional dictums concerning the design of a national UPI system to the patient community without respect in allowing the patients to comprehend the system's full functionality and design will have a negative effect on continuation intent of utilizing any proposed national UPI system. This inference has now been clinically tested and researched.

In Akter, Ambra, & Ray's (2011) study of trustworthiness in mHealth systems, a focus was placed on defining and measuring continuance intentions of using a particular mHealth system. They measured **ability**, **benevolence**, **integrity**, and **predictability** of mHealth services. Their study found that ability and integrity were relatively more important than the others; yet, a deflating rating in any of the four would constitute a reduction in all the measured factors (Akter, Ambra, Ray, 2011). This breakthrough study shows the very characteristics that must be present in any UPI system. Any lack of these factors, and the system's trust perception will plummet. Based on the empirical evidence of the India UID effort, it is clear that these four factors were absent or limited in perception in the minds of the patients.

Another study by Akter & Hani (2011) affirms the four factors of Akter, Ambra, & Ray (2011) by correlating patient satisfaction with overall healthcare service. This means that in the mind of the patients, satisfaction is derived from "good" customer service (Akter & Hani, 2011). As is the case in all other industries, in a capitalistic society, "good" is defined by competitive economic market forces driving the need for organizations to offer the best clinical information and treatment options to their patients. Anything less will result in a failed attempt to attract patients into utilizing that healthcare provider's medical services.

The previously discussed research on measurable trust factors describes patient expectations that could lead to possible national UPI design considerations that would avoid the pitfalls of the opponent's arguments; therefore, this research review will offer a hypothetical design concept of a patient knowledge empowered based national UPI system.

Is there a way to get the benefits of a national UPI without creating a new US federal infrastructure or department?

As previously discussed in Akter, Ambra, and Ray's (2009) research, **ability**, **benevolence**, **integrity**, and **predictability** are the key factors that must be present in a trusted mHealth system. One could make the argument that mHealth technology uses the same core IT systems as most other mobile technologies. This review makes the assumption that healthcare system users perceive the benefits of mobile devices over stationary equivalents in the same manner overall, so discussing any mobile Internet based technologies includes mHealth as well.

In 2008, Rand Corporation sponsored an extensive study researching effective system designs for UPI system in the US (Hillestand, Bigelow, Chaudhry, Dreyer, & Greenberg, et al, 2008). Three comprehensive systems were proposed by Hillestand, Bigelow, Chaudhry, Dreyer, & Greenberg, et al (2008). The three systems were proposed as follows: 1) Access Provider System. 2) National system that accesses payer-held data 3) Personal Health Records. Each solution put the patient in charge of the data and the ability to access it. The conflict in the system was the physician was obligated to contact the patient for permission when records were needed. This slowed the process down, and used up valuable physician diagnosis time (Hillestand, Bigelow, Chaudhry, Dreyer, & Greenberg, et. al, 2008).

Allowing the patient to trust the performance of the system (*ability*), perceive an actual health benefit from the use of the system (*benevolence*), trust that the information was accurate and secure (*integrity*), and feel assured that accessing the data was a consistent repetitive and stable experience (*predictability*) seems to be the right combination necessary for all parties involved to agree on a national UPI systems. The answer may be private Health Information Exchange (HIE) providers.

PROPOSED SOLUTIONS

Only in the last few years has information technology advanced to the point that large amounts of medical information can be accessed by the general population in an efficient and easily acceptable format. The technology that drives this is cloud computing and mobile technology. According to comScore, a recent study confirms this claim (Cocotas, 2012, February 15).

If we can combine cloud computing, mobile technology, a market-based patient information dissemination system, and extend the patient trust model of Akter, Ambra, and Ray's (2009) mHealth devices research to an entire centrally designed national UPI system, the benefits of such a system may justify the relenting of the opposition's position.

Health Information Exchanges

In terms of ability, Kaiser-Permanente has combined their financial and healthcare system together (Frisse, 2011). This proves that a commercial entity can cost effectively provide patient information to its healthcare providers. This type of system is prevalent in Europe (Frisse, 2011).

The US Department of Health and Human Resources could outsource to private companies that provide a voluntary patient participated Health Information Exchange (HIE) service. Their only charter would be to hold any patient's medical data in escrow, synchronize the data between all HIE participating service providers, and act as licensed (benevolent) guardians of the data on behalf of all US patients across the country. Any patient could determine what data was exposed at what level, and not be concerned that third-parties could access data without permission. This predictability in the service would allow for a confidence to ensue in the entire patient community.

HIE Transmission Security Concerns

What if there was a breach? Under this proposed concept, legislation could be enacted that made it a federal crime for an HIE organization to disclose patient information. Breach of this trust could be a US felony crime with criminal and civil penalties. That would bring integrity to the system and severe consequence would be incurred if the patient community's trust was violated. Assuming that a breech was not intentional by the HIE service providers, what technologies could be incorporated in the system's design to thwart a major security breach? The key is to simplify the transaction channel between HIE providers. Standardization of systems across all HIE organizations will alleviate bottlenecks and incompatibilities found in the current system.

Integrating Accepted Industry Standards

This is not a new concept. The HL7 organization has organized the standardization interoperability between healthcare providers since 1987 (Terry, 2012, September 5). Now they are making their core protocol "open source" and allowing it to be utilized across dissimilar systems without licensure (Terry, 2012, September 5). This means that the core protocol that has been used for many years by healthcare providers throughout the US can be incorporated without a fee to every organization in the healthcare industry. Software technologies such as the University Health Network (n.d.) of Toronto, Canada's HAPI java HL7 parser and Mirth, an open-source cross-platform HL7 interface engine, is taking advantage of the announced open-source HL7 protocol release (Elyse, 2006, April 20).

There may be concerns that all of the HL7 protocol iterations are primarily designed at the OSI Application layer. Standardizing on IPv6 for the HL7 protocol could go a long way in providing inherent security in data transmission between HIE sites (Hermann-Seton, 2002). In a recent letter to Justine Carr, M.D., Chairperson of the National Committee on Vital and Health Statistics, Kathleen Sebelius, the Secretary of Health and Human Services, agreed with Dr. Carr concerning the need to nationally "streamline health care transactions and operations" (Sebelius, 2012, July 6). This proves there is a viable network of interest at the federal government level as well as the healthcare provider level for standardization.

This research and professional interest in streamlined interoperability proves that the information technology data channel, not the technology endpoints should be the focus of any UPI national system design. Harris & Alter (2010, January) of Accenture have defined the top security risks for any cloud computing effort as follows: loss of governance, lock-in, management interface compromise, data protection, isolation failure, compliance risks, malicious insider attack, and insecure or incomplete data deletion.

The Need for Centralized Design

Most of these risks center on the focus of a single 'cloud' service provider. If the federal government defines the operation of the HIE organizations, all would be identical in their operation and security procedures. This would lead to more efficient and secure interoperability between many HIE providers. This is no different than the deregulation of the natural gas markets in many states. One provider offers the commodity of natural gas, while several commercial entities provide the billing services. The federal government in this case would provide the design standards, and the HIE service providers would provide the day to day operations for UPI patient services.

The costs would be incurred by the patient as an additional insurance premium federal charge, similar to FCC regulation fees currently charged to a telephone user. Also, since it is a voluntary service, many health insurance providers, or healthcare exchange co-ops, may offer the service at no charge due to the added savings generated by such a system since their information technology costs could be outsourced to the HIE providers.

Cloud Technology Implementation

Now that the channel has been secured by IPv6, and the industry has standardized on HL7 protocol for data transmission, the last step is the client-server communication. That should be handled by today's cloud technologies.

It is clear that mobile technology is the future of IT in many industries - no less in the healthcare industry. Guo, Sun, Yuan, Yan, & Wang (2012, July, 11) researched the mediating role of trust in mobile health technologies. Their research showed that perceived privacy violation was a deterrent of trust and behavioral intention. (Guo, Sun, Yuan, Yan, & Wang, 2012, July, 11). Based on this research, the HIE system will provide confidence in patients not only because they will have legal protection from fraud, but also patient transferability rights in provider choice may be invoked if the current HIE customer service is poor. Why, because there will be multiple HIE providers from which to choose. This directly correlates with market behavior. Since mobile technology is ubiquitous today, changing HIE providers could be done with a touch of virtual button on a patient's mobile device.

How would the UPI be used in the medical environment? Using an NGN/IMS system with cloud computing to reduce the burden of organizing and improving the functions of existing mobile health monitoring systems, the patient's UPI number could be hashed by the HIE service provider, transmitted via the Internet, and then utilized by a physician using their own physician's code in the HIE system. This would protect all patients' UPI number's security integrity during transmission.

Only professionals that are authorized to perform certain procedures would be able to access HIE resources based on need. Passing that information to unauthorized third-parties would mean loss of a doctor's license to practice medicine (Nkosi & Mekuria, 2012). Medical procedures only authorized by the physician's HIE code combined with the patient's hashed UPI number would allow for medical devices to function, data to be transmitted, or prescriptions to be ordered. All of this is transported via cloud technologies with a secure HL7/IPv6 transmission protocol.

Public policy concerning cloud technology security has been clearly defined by NIST (Jansen & Grance, 2011, December, 14). They have defined what is and is not secure for cloud providers. By allowing the US Government to license private HIE entities to offer secure patient and medical professional access to critical medical data will bring forth a more secure healthcare environment over all. It would not be too difficult to specify the correct procedures for utilizing a national standard UPI system nationwide. The technologies are already available, and are already industry standards.

Several studies on doctor-patient trust clearly show that only trust of the system by the patient will lead to a cooperative behavior between patient and doctors and the systems they utilize to communicate most effectively (Klein, 2007). The key is a UPI number that is controlled by the patient, combined with a UPI system that allows them to control which healthcare professional or entity has access to an appropriate level of the patient's data. It is clear that the healthcare industry can no longer consider patients' records their property. The records belong to the patients, and it is incumbent upon the patients to make sure their records are safe. Only the US Government has the jurisdiction to allow for a national effort to streamline our current system nationwide.

Thanks to cloud technologies, the patients would have total control of the information, but physicians could contact health professionals at any participating HIE when technical information was necessary. These HIE's would be staffed by licensed medical professionals that could manage the data requests appropriately. Synchronized data between the HIE providers would go a long way in satisfying a national need for a single point of access, with the added bonus of patient records controlled by the patient. By decentralizing the UPI depository, patients could participate in any HIE and still have national coverage. All the factors that determine trust in a mHealth environment, namely, ability, benevolence, integrity, and predictability are accommodated with this solution.

The key to success for this proposed national UPI system implementation requires a patient controlled UPI number that securely connects a national specification mandated US Government network and decentralized HIE service providers.

CONCLUSION

This study's evaluation of a recently attempted national UPI system in India, and its implementation failure, combined with several research studies from the UK and US, has concluded that a lack of patient trust factors in UPI design is the major flaw that led to the India UID implementation failure. This paper proposes the "next" logical step, which is to create a national UPI system based on a patient trust model design. This study has taken the steps necessary to expose the critical factors to create such a research study. It is hoped that this study will inspire further research into designing a cloud computing based, patient trust focused, national Health Information Exchange network that manages a US national UPI standard.

REFERENCES

1. AHIMA. (2009, July) Managing the integrity of patient identity in health information exchange. *Journal of AHIMA.* 80 (7). pp. 62-69. Retrieved November 8, 2012 from http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_044000.hcsp?
2. Akter, S., D'Ambra, J., & Ray, P. (2011). Trustworthiness in mHealth information services: An assessment of a hierarchical model with mediating and moderating effects using partial least squares (PLS). *Journal of the American Society for Information Science and Technology*. 62(1). pp. 100 – 116. John Wiley & Sons, Inc.: New York, NY. Retrieved November 11, 2012 from http://ehis.ebscohost.com.proxygsu-sct1.galileo.usg.edu/eds/pdfviewer/pdfviewer?vid=4&hid=101&sid=a4181515-c184-4f7c-8ed1-dbf7c223c51b%40sessionmgr113
3. Akter, S., Hani, U. (2011). Modeling the effects of quality in a transformation health service. *Unpublished document from ANZMAC 2011*. Melbourne, AU. Retrieved November 12, 2012 from http://anzmac.org/conference/2011/Papers%20by%20Presenting%20Author/Akter,%20Shariar%20Paper%20111.pdf
4. American College of Cardiology Health IT Committee (n.d.) Unique patient identifier principles. *American College of Cardiology*. Retrieved November 8, 2012 from https://www.cardiosource.org/Advocacy/Issues/Health-Information-Technology/ACC-Policies-and-Activities/Unique-Patient-Identifier-Principles.aspx
5. Brase, T. (2012). National Patient ID. Retrieved December 26, 2012 from http://www.cchfreedom.org/files/file/Final_UPI_Report-Use%281%29.pdf
6. Cocotas, A. (2012, February 15). The fastest-growing mobile web category is health information. *Business Insider: BI Intelligence.* http://articles.businessinsider.com/2012-02-15/research/31062144_1_mobile-health-mobile-web-smartphone-sales
7. Collins, M. & Peel, D. (2012, January 23). Should every patient have a unique id number for all medical records? *Wall Street Journal.* Retrieved November 8, 2012 from http://online.wsj.com/article/SB10001424052970204124204577154661814932978.html
8. Doyle, J., (2012, October 28). Nhs lost track of 1.8m patient records in a year with sensitive information found in public bin and for sale on the internet. *MailOnline.* Retrieved January 2, 2012 from http://www.dailymail.co.uk/health/article-2224580/NHS-lost-track-1-8m-patient-records-year-sensitive-information-public-bus-sale-internet.html
9. Elyse. (2006, April 20). Mirth: An open source cross-platform hl7 interface engine [Web Page]. Retrieved November 13, 2012 from http://www.anticlue.net/archives/000683.htm
10. Frisse, M.E., (2011). Health information exchange in memphis: impact on the physician-patient relationship. *Journal of Law, Medicine & Ethics*. 38 (1). pp 50 – 57. Retrieved November 12, from http://www.ncbi.nlm.nih.gov/pubmed/20446983
11. Guo, X., Sun, Y, Yuan, J., Yan, Z., & Wang, N. (2012, July, 11). Privacy-personalization paradox in adoption of mobile health Service: The Mediating Role of Trust. *PACIS 2012*. Retrieved November 12, from http://pacis2012.org/files/papers/pacis2012_T3_Guo_300.pdf
12. Hermann-Seton, P. (2002). Security features in ipv6. *SANS Reading Room: GIAC GSEC Practical Assignment v1.4, Option 1*. pp 17. Retrieved November 20 from http://www.sans.org/reading_room/whitepapers/protocols/security-features-ipv6_380
13. Harris, J. & Alter, Allan E. (n.d.). Six questions every health industry executive should ask about cloud computing. *Accenture Institute of Health and Public Value* [Brochure], New York, New York: Wan, D., Greenway A., Harris, J. & Alter, A. Retrieved November 8, 2012 from http://www.accenture.com/us-en/Pages/insight-cloud-computing-six-questions-summary.aspx
14. Hillestand, R., Bigelow, J., Chaudhry, B., Dreyer, P., Greenberg, M., Meili, R., Ridgely, M., Rothenberg, J., & Taylor, R. (2008). *Identity crisis: An examination of the costs and benefits of a unique patient identifier for the u.s. health care system.* Santa Monica, CA: RAND Corporation. Retrieved November 13, from http://www.rand.org/content/dam/rand/pubs/monographs/2008/RAND_MG753.pdf
15. Hu, X., Bell, R., Kravitz, R., & Orrange, S. (2012). The prepared patient: Information seeking of online support group members before their medical appointments. *Journal of Health Communication: International Perspectives*, 17(8). pp. 960 - 978

16. Jansen, W. & Grance, T, (2011, December, 14). Guidelines on security and privacy in public cloud computing. *NIST: Special Publication.* pp. 800-144. Retrieved November 13, 2012 from http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf
17. Kakkar, M. (2011, December 14). India's unique id project all but dead [Web Page]. *ZDNet*. Retrieved November 14, 2012 from http://www.zdnet.com/blog/india/indias-unique-id-project-all-but-dead/802
18. Klein, R. (2007). Internet-based patient-physician electronic communication applications: patient acceptance and trust. *e-Service Journal*. 5 (2). pp. 27-51. Retrieved November 13, 2012 from http://ehis.ebscohost.com.proxygsu-sct1.galileo.usg.edu/eds/pdfviewer/pdfviewer?vid=2&hid=23&sid=691b2a98-d17b-4acd-9cab-7bb24ec6feb9%40sessionmgr13
19. Nkosi, M.T. & Mekuria, F. (2012). Cloud computing for enhanced mobile health applications. *2nd IEEE International Conference on Cloud Computing Technology and Science (CloudCom 2010)*. p5. Indiana University, USA. Retrieved November 8, 2012 from http://researchspace.csir.co.za/dspace/bitstream/10204/4767/1/Nkosi_2010.pdf
20. Palmer, E. (2012, July 5) FDA gets device, but not drug tracking. *FiercePharma Manufacturing*. Retrieved November 8, 2012 from http://www.fiercepharmamanufacturing.com/story/fda-gets-device-not-drug-tracking/2012-07-05
21. Parker-Pope, T. (2008, July 25). Doctor and patient, now at odds. *New York Times*: *Well*. Retrieved November 13, 2012 from http://www.nytimes.com/2008/07/29/health/29well.html?_r=2&
22. Rowe, R. & Calnan, M., (2006, February). Trust relationships in healthcare – the new agenda. *European Journal of Health Law*. 16 (1). p. 4-6. Retrieved November 13, from http://eurpub.oxfordjournals.org/content/16/1/4.full
23. Rynning, E. (2007, July). Public trust and privacy in shared electronic health records. *European Journal of Health Law*. 14(2) pp. 105 -112. Retrieved November 12, 2012 from http://ehis.ebscohost.com.proxygsu-sct1.galileo.usg.edu/eds/pdfviewer/pdfviewer?sid=9e81d37f-3113-4924-ba71-e486ac86550c%40sessionmgr15&vid=3&hid=23
24. Saenz, A. (2010, September 13). India launches universal id system with biometrics. *SingularityHUB*. Retrieved November 8, 2012 from http://singularityhub.com/2010/09/13/india-launches-universal-id-system-with-biometrics/
25. Sebelius, K. (2012, July 6). Process for developing, maintaining, and updating standards and operating rules. *US Department of Health and Human Resources*. p 2. Retrieved November 14, 2012 from http://www.ncvhs.hhs.gov/120706lt.pdf
26. Terry, K. (2012, September, 26). Himss asks congress for patient identity system – again. *InformationWeek.* Retrieved November 15, 2012 from http://www.informationweek.com/big-data/news/healthcare/patient/himss-asks-congress-for-patient-identity-systemagain/240007949
27. Terry, K. (2012, September, 5). Hl7 to offer messaging standards as freebie. *InformationWeek*. Retrieved November 14, 2012 from http://www.informationweek.com/healthcare/interoperability/hl7-to-offer-messaging-standards-as-free/240006730
28. University Health Network. (n.d.). HAPI: the free, open, and best hl7 parser and library for java [Web Page]. *University Health Network*. Retrieved November 12, 2012 from http://hl7api.sourceforge.net/
29. WHO. (2007, May). Patient identification. *WHO Collaborating Centre for Patient Safety Solutions.* 1(2), p. 4. Retrieved November 13, 2012 from http://www.ccforpatientsafety.org/common/pdfs/fpdf/presskit/PS-Solution2.pdf