Challenges of Challenges of Deploying RFID Technology for Reducing Medical Identity Theft

Phillip Leicester, Siddhivinayak Kulkarni
School of Science, Information Technology and Engineering
University of Ballarat, P. O. BOX 663, Ballarat, Victoria, 3353, Australia

Abstract

The healthcare industry is the biggest user of RFID technology due to its mobility in delivering data, tracking and surveillance of every individual, pathology tests, medications and the management of patient data. Because this technology is so vital within the healthcare/hospital environment this paper investigates and analyses the challenges as well as the issues facing RFID technology in implementing and providing security in guarding against the occurrences of medical identity theft. This form of identity theft is life threating as it adds medical data to a patients file who didn't receive treatment for whatever conditions the imposter obtained as a result of their criminal activity. In preventing medical identity theft requires specific proposals from a policy, social and technological perspective.

1. Introduction

The purpose of this research paper is to conduct an investigation and analysis on the challenges and issues confronting RFID technology in being implemented as a technological security mechanism in dealing with medical identity theft by addressing my question on, "RFID proposals in preventing medical identity theft?"

Medical identity theft is another form of identity theft that is relevantly new and ever increasing as this recent form of criminal activity as yet has neither definitive legal definition nor recognition within any Federal or State criminal statute due to its hidden nature.

But unlike other criminal activities of identity theft, medical identity theft has the potential to kill or inflict serious illness to those who have had their medical records comprised without their knowledge. In order to combat this form of identity theft I will explain what Radio Frequency Identification (RFID) technology is and what needs to be accomplished in order for this technology to be safely used in preventing medical identity theft.

2. RFID Technology

Radio Frequency Identification (RFID) technology is predominantly used within the transport and logistics sector, but its applications has continuously been accepted by other organisational and government sectors as well, with the healthcare industry being the third highest to incorporate this technology.

Its technology consists of a tag, a transmitter that sends and receives radio signals and a scanner used for tracking an object from point A to point B throughout the entire process. The tag contains a software chip that has within it vital information about the object itself that it is placed upon, as well as an antenna that will enable a radio transmitter to track the signal being emitted from the tag. The electronic product code (EPC) refers to a unique identifier, just as a primary key would be used within a database that is built into the tag for identification purposes including additional functionality such as read/write storage, encryption, control access and integrated sensors used for detection. Each EPC contains the following elements within it namely a header, a filter value partition, an EPC Manager (refers to company prefix), an object class (item reference) and a serial number with all elements of the EPC totalling 44 bits [16].

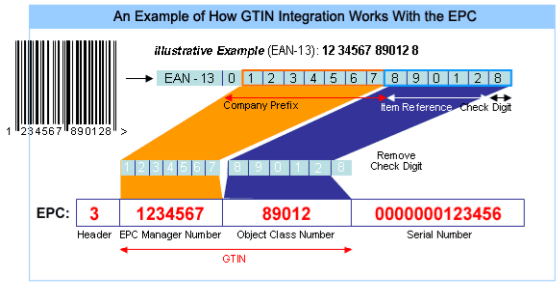

Figure 1. EPC Data Overview [17]

Once the object containing the placed RFID tag is within range of the scanner (reader), the scanner then proceeds to transmit an electromagnetic field that unites the antenna with the tag, whereby energy immersed from the electromagnetic field is used to power the software chip contained within the tag to enable modulation of the radio frequency that corresponds with the tags EPC and software code.

The scanner then proceeds to decode information stored within the transponder as soon as the modulated signal is located by the scanner where information is then relayed to a computer whereby the processing of information occurs and is stored. [5, 8]

The following diagram illustrates the operability of an RFID system as indicated.

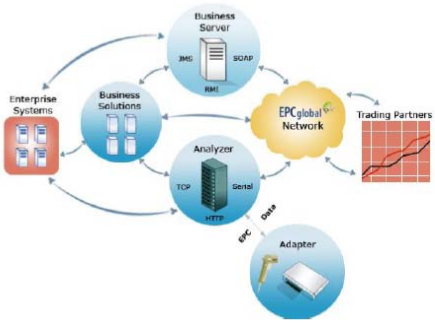

Figure 2. Typical RFID System Overview [18]

The disadvantages of RFID technology include the following:

- Signal strength limited to a required distance;
- Radio frequency unable to work in certain geographical areas;
- Electromagnetic field prone to interruption from solar and electrical storms.

The medical and healthcare sectors are using this technology as a means to keep track of medical equipment and the delivery of pharmaceuticals that proved to be costly in the past when it came to tracking them down. But now this technology is being applied as a means of protecting online medical information systems from those who are involved in perpetrating the criminal activity of medical identity theft. Because the identity of every individual is centred around recognising specific features, personality, knowledge and traits that define who we are requires having the implementation of a robust identity management system that can be used in determining our individual specific features and characteristics through the provision of unique identifiers in recognising us. [10]

This is where RFID comes to the fore as part of its functionality is to provide identification through the use of unique identifiers (EPC) that are embedded within every RFID tag; the same uniqueness that identifies us could be stored in individual EPC's within every tag. The problem though regarding this form of identification refers to the non-uniformity of RFID standards; standards which need to be implemented immediately as they are a necessity for the operation of an identity management system in ensuring accuracy and data reliability are constantly maintained. By having standards of uniformity for RFID applications will systematically reduce costs and establish technological requirements in the manufacturing of RFID chips, readers and all relevant hardware/software including system maintenance [8, 10]. Also RFID uniform standards would enable the difficulties in relation to security in being addressed as this is one of the concerns that this technology has to overcome in order for it to restrict comprised abuse in accessing medical information and it must be cost effective in providing security necessity. The moment the cost of implementing security measures within RFID technology, namely the tags, causes the price of this technology to soar then many private and government organisations will look at alternative technologies in providing wireless or fixed security measures that won't erode their IT budget as all organisations have budgetary constraints that they have to deal with throughout each financial year. [5]

Another problem that RFID technologies has to contend with is privacy, which is another reason why the introduction of uniform standards is vital for if this technology is unable to sustain our privacy then this technology will lose customer confidence, which would set it back as a reliable technology.

Furthermore, the relaying of information from the RFID scanner to the computer will require the implementation of data management procedures to solve problems associated with multiple tag readings and dirty data as data accuracy is paramount when processing patient and medical information as this information deals with the lives of patients seeking medical treatment that would ultimately have dire consequences on those patients if the accuracy of such data was unreliable to begin with.

3. RFID Middleware

In addition to solving data management issues, the issues involving the management and removal of redundant data will effectively need the use of utilising a middleware management environment in handling and organising the large volumes of data that are emitted from numerous RFID tags for the purposes of establishing data accuracy and data validity within the RFID system environment [4, 6, 7].

Currently all RFID systems rely upon the use of middleware architecture as a means to interface with operating platforms and their various information systems as this middleware is the functioning nervous system that is central to all RFID operations. Its direct purpose is to undertake the management, filter, process and monitor the gathering of all information retrieved from RFID readers whereby the information is then routed onto numerous information systems utilising enterprise resource protocols. [5]

There are however numerous challenges that must be overcome that pertain specifically to the use of RFID middleware as it provides the main communication corridor between the RFID network and the databases of the healthcare/hospital network and patient management systems. These challenges comprise the establishment of middleware uniform standards, the reduction of costs associated with

hardware, security/privacy concerns, as well as the merging of RFID systems with current information system infrastructures in maintaining complete data reliability/integrity and the data management of massive voluminous size that RFID systems have a tendency to initiate.

There are four layers that interact with each other within the RFID middleware architecture that consist of the following: - Device, Edge, Enrichment and Application layers.

The Device Layer consists of RFID tags/readers which provide the necessary fast connection to the RFID readers that enable medical applications performing within hospital systems in accessing the retrieval of data through the filtering and clustering of raw information obtained from RFID readers. The Edge Layer deals with device controllers that form part of the reader software used for filtering the data stream by preventing duplication and read errors. The Enrichment Layer is responsible for preparing information from device controllers in being readily available for use by high-level applications whereby business processes occur that allow real-time amalgamation with existing hospital systems. The Application Layer utilises applications that interact with the RFID data, as well as ascertaining an application level connection with the Device Layer that specifically necessitates the reader management and processing of numerous volumes of RFID data required for medical applications [11, 16].

The diagram below illustrates each of the 4 layers that comprise middleware architecture.

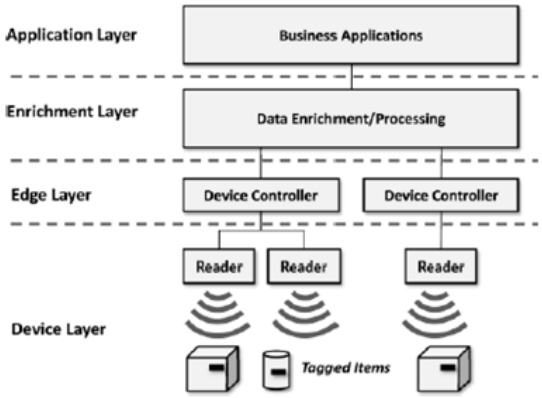

Figure 3. RFID Middleware Layers [16]

A detailed layout of an RFID Health Information System performing within a hospital environment is illustrated below showing why this technology is attracted by and actively sought after by hospital administrators.

Figure 4. RFID Health Information System [19]

The benefits for hospitals in having an RFID wireless information system refers to its internal network infrastructure being geographically confined to the hospital itself. You will also notice that its internal wireless network is linked to an external fixed cable Wide Area Network (WAN) in relaying information to other organisations in the external world. [3, 9]

It will also provide the following applications that hospitals rely upon.

- Tracking of Patients/Staff
- Tracking of hospital assets
- Tagging of pathology/lab samples
- Management of blood products
- Medical implants containing patient medical history
- Inventory of pharmaceuticals/medications
- Management of Operating Theatre/Intensive Care Unit (ICU)
- Management of sterilisation processes

4. RFID Security

When dealing with any form of identity theft especially medical identity theft a crime that affects the elderly, the chronically ill, as well as those who require access to the health system on a regular basis are the most vulnerable as the security measures implemented by the healthcare industry failed to protect them due to inadequate policies or weren't acceded to by minority healthcare organisations.[12] In the United States the Health Insurance Portability and Accountability Act (HIPAA) restricts access rights to individual health files, thus preventing the eradication of any false information. According to Pam Dixon, Executive Director of the World Privacy Forum their needs to be an established national standardised procedure implemented within the United States where policies are concerned in dealing with medical identity theft. Technological security alone cannot stifle medical identity theft for it requires the implementation and enforcement of policy procedures which must involve the consensus of insurance organisations, stakeholders, representatives of patients/consumers and medical administrators to determine policy outcomes. [1, 13]

As mentioned previously due to the fact that some healthcare organisations failed to adhere to the security and privacy measurements of the (HIPAA) the American Recovery and Reinvestment Act (ARRA) has acquired additional enhancement of its rules that enable the allocation of more stringent penalties and enforcement that will see more healthcare organisations in the United States and the professionals who work in these environments being more responsive towards their data security efforts. [13]

In preventing medical identity theft some hospitals in the United States have undertaken a two-way frontal attack through the utilisation of passive RFID devices in conjunction with biometric systems in identifying fingerprint and iris patterns or vein patterns of the palm thus providing a formidable barrier against medical intrusion. Many software organisations are currently designing new software applications that will have the capacity to detect possible medical identity theft occurrences through the installation of software on hospital computers that will scan any unusual activity and notify of any other breaches of the system as discovered by Howard J. Anderson reporting for the Health Data Management Magazine. [13]

Another challenge facing RFID security is the thought of combining RFID technology with biometric technology to reinforce the accuracy and security in delivering biometric identification, as well as data obtained from an RFID device, but in order for this to occur would require ongoing social acceptance of both these technologies in delivering their expected performance outcomes. Only then when society as a whole can accept these technologies as an equipped tool in securing their identities from the criminal element instead of allowing their perception and scepticism in fearing these systems as a means of invading their privacy. Having the combination of biometrics and RFID being simultaneously linked to every individual database that is connected to a central database would subsequently provide a much more efficient system in determining the identity and location of every individual within the hospital environment. With the ongoing technological advancements of these emerging technologies all governments of developed countries and their various industries are more likely to co-operate with each other in sharing and collecting relevant data on a real-time basis as suggested by “Christie Perakslis and Robert Wolk” respectively.[14]

The most likely RFID application to be used in preventing medical identity theft is a mobile application developed by the VeriChip Corporation in the form of an implanted microchip within each human being positioned just under the skin in the upper forearm. However, the use of having an implanted chip within a human being conjures up an ethical dilemma amongst bioethical councils and philosophers. But do the negative concerns of this technology really outweigh the positives as being a formidable RFID security solution in combating medical identity theft and ensuring patient identification. This is a natural occurrence that is directed towards the development and implementation of any new technology, especially where the protection of securing personal and organisational data is concerned. The ability to accurately identify every patient staying in hospital is of paramount importance as errors with patient identification can have drastic consequences, such as improper dosage of medications, surgical procedures performed on the wrong patient, inaccurate test results and pathological lab work performed resulting in medical misdiagnoses and vital medication errors which RFID technology can reduce, as well as ensuring patient care and security. [12, 15]

The VeriChip Corporation is a subsidiary of the Applied Digital organisation that is responsible for the development of the current RFID security technologies used to identify, track and protect citizens and their property. Their directive is dedicated towards being the foremost leader of RFID systems within the field of healthcare and has commenced making hospitals aware of their VeriMed Patient Identification System which contains a unique 16-digit identification number that can be scanned to identify a patient and their medical history in expediting treatment as quickly as possible. The applications for this technology are immense, but from a security perspective this human-implantable technology has the capacity to provide protection at a level thought to be inconceivable as stipulated by Adnan F. Kocamaz and Erdem Ucar. With this technology hospitals and other healthcare organisations will be able to secure specific areas by interfacing it with their existing systems, thus enabling the tracking of every individual and object in real-time. [15]

Below is an illustration that depicts the operational function of the VeriChip.

Figure 5. VeriChip System Schematic [20]

As far as Australia is concerned the best way in tackling medical identity theft is through the implementation of national health policies and ongoing technological infrastructure. In 2007 the then Prime Minister of Australia Kevin Rudd announced a new e-health bill that would entail the delivery of a 16 digit ID Medicare number to every Australian as from the 1st July, 2008 in ensuring that all available healthcare treatment was being given to the correct individual through the matching of information on the Medicare computer system. However, privacy advocates claimed the e-health bill that was being introduced by the federal government would violate portions of the privacy act as the enactment of the bill would be directed towards the provision of RFID implanted microchips.

The manufacturer of these implants PositiveID also known as the VeriChip Corporation in the United States claims that they will greatly reduce the incidents of credit fraud, including medical identity theft which currently affects 7 per cent of the Australian population and that the use of these implants have existed for some time now in the United States, even though some privacy advocates within the United States have also voiced out their concerns involving this form of technology. [2] The Chairman of PositiveID Scott R. Silverman has acknowledged that patients will solely remain in control for their own health information through the establishment of a robust patient oriented interface though the critics of this system aren't convinced that will be the case. The reasoning behind Medicare utilising a 16 digit number refers to the fact that the PositiveID microchip relies upon the use of a 16 digit number as an identifier to provide a connection to the medical database that stores the patient's personal and medical information. It is interesting to note that IBM has continually funded PositiveID since it was founded and that Medicare has always maintained a healthy relationship with IBM as Medicare's entire technological infrastructure utilises IBM equipment and they have decided to extend their contract arrangements with IBM that is valued in the vicinity of $189 million that will result in the ongoing commercialisation in driving the continual utilisation of this technology. At the moment it is important to recognise that this e-health bill is still before the Australian senate recommending against having RFID implants as being a mandatory requirement and as yet they are still to hand down their decision on the matter [2].

5. Conclusion

Medical Identity Theft is a relevantly new form of identity theft that has just begun to affect patients, hospitals and health insurance organisations alike; costing millions of dollars in the United States where it all began and is slowly spreading its criminal activity to other western countries including Canada, United Kingdom and Australia. But unlike other forms of identity theft, medical identity theft can inflict death on those whose medical records have been comprised with the perpetrators medical information being stored within the victim's file. It is also a crime that is considerably hard to detect as the perpetrators infiltration of a particular patient's medical file is stealthily hidden amongst the large volumes of medical information stored within the system.

The solution to minimising medical identity theft and the protection of all medical records can be instigated through the utilisation of RFID technology; a technology that has evolved considerably from its supply chain environment to the healthcare environment as part of its ongoing computerisation of the entire healthcare system. But in order for RFID technology to be successful in combating medical identity theft there needs to be global uniformity of the technology itself and its operational capacity to deliver high security functionality, as well as overcoming issues involving privacy. Furthermore, a robust middleware management system will be required to handle all dissemination and filtration of data, as well as complete system interoperability with other system platforms and devices that will ensure complete system stability and performance in dealing with large volumes of various healthcare information.

The other challenge that needs to be overcome is the challenge of social acceptance of RFID technology as a security application in protecting all personal and medical information within a hospital environment as scepticism and fear of this technology breeds ignorance which can only be eliminated through well informed information and education.

6. References

[1] "Dixon, Pam." (2007). Medical Identity Theft: Issues and Responses, pp1-8.

[2] "Greg Nikolettos" (2010). Kevin Rudd's e-Health Bill paves the way for PositiveID Human Implantable RFID Microchips. Retrieved August 9, 2010, from http://www.opednews.com/articles/Kevin-Rudd-s-e-Health-bill-by-Greg-Nikolettos100408839.html.

[3] "Mundra, Shivam" (2007) RFID and Its Applications in Healthcare Retrieved October 10, 2010 from http://www.health-beat.blogspot.com.

[4] "Christian Floerkemeier," "Lampe, Matthias" (2005). RFID Middleware Design Addressing Application Requirements and RFID Constraints., pp219-224.

[5] "Linda Castro", "Samuel Fosso Wamba". (2007). AN INSIDE LOOK AT RFID TECHNOLOGY. Vol 2 (1), pp128-141.

[6] "Hee Joung Hwang", "Jin Tak Choi". (2007). Design of an aspect-based framework to improve the dynamic management of RFID middleware, pp1-6.

[7] "Ahmed, N.," "Kumar, R.," "French, R. S., & " "Ramachandran, U. (2007). RFID: A Reliable Middleware Framework for RFID deployment, pp1-10.

[8] “Suhong Li”, “Visich, John K.”, “Khumawala, Basheer M.”, “Zhang, Chen” (2006) "Radio Frequency Identification Technology: Applications, Technical Challenges and Strategies", Sensor Review, Vol. 26 (3), pp.193 – 202.

[9] “Wicks, A. M.”, “Visich, J. K.”, “Li, Suhong” (2006). Radio Frequency Identification Applications in Hospital Environments. Hospital Topics, Vol 84 (3), 3-9.doi:10.3200/HTPS.84.3.3-9.

[10] “Pfitzmann, Andreas” (2009) Identity Management pp1-32.

[11] “Chowdhury, Belal”, “Khosla, Rajiv” (2007) RFID-Based Hospital Real-Time Patient Management System, pp1-6.

[12] “Cerlinca, Tudor Ioan”, “Turcu, Cristina”, “Turcu, Cornel”, “Cerlinca, Marius” (2010). RFID-based Information System for Patients and Medical Staff Identification and Tracking, pp193-206.

[13] “Anderson, Howard J.” (2010). User Authentication Strategies, pp.1-4.

[14] “Perakslis, Christine”, “Wolk, Robert” (2006). Social Acceptance of RFID as a Biometric Security Method, pp. 34-42.

[15] “Kocamaz, Adnan Fatih”, “ Uçar, Erdem” (2009). A RFID Application About Health Imformation Mobile Aplication: Verichips, Vol. 7, Suppl. 2, pp100-105.

[16] “Evdokimov, Sergei”, “Fabian, Benjamin”, “Gunther, Oliver”, “Ivantysynova, Lenka”, “Ziekow, Holger” (2010). RFID and the Internet of Things: Technology, Applications, and Security Challenges, Vol 4 (2), doi: 10.1561/0200000020, pp105-185.

[17] “The Consumer Goods Forum” (n.d). Connected Business Information: Electronic Product Code. Retrieved September 20, 2011 from http://www.globalscorecard.net/live/guide_to_ecr_cbi03.aspx.

[18] “Supply Insight” (n.d). rPlatform – The RFID Platform. Retrieved September 20, 2011 from http://www.supplyinsight.com/rplatform.htm.

[19] “ITGS Online” (n.d). RFID Technology in a Medical Setting. Retrieved September 20, 2011 from http://itgsonline.com/?p=100.

[20] “free-forums.org” (2000). How does a VeriChip System Work. Retrieved April 25, 2012 from http://www.noidchip.free-forums.org/department-of-engineering-physics-verichip-report-vt153.html.

