CONSUMER PERSPECTIVES OF IMPLANTED RADIO FREQUENCY IDENTIFICATION (RFID) DEVICES FOR MEDICAL INFORMATION RETRIEVAL

Andrew S. Jensen
Department of Computer Science
University of North Carolina at Charlotte
Charlotte, North Carolina 28223
ajensen7@uncc.edu

Joseph A. Cazier
Department of Computer Information Systems
John A. Walker College of Business
Appalachian State University
Boone, North Carolina 28608
cazierja@appstate.edu

Dinesh S. Dave
Department of Computer Information Systems
John A. Walker College of Business
Appalachian State University
Boone, North Carolina 28608
daveds@appstate.edu

ABSTRACT

Many organizations are adopting radio frequency identification technologies (RFID) as part of their information supply chains for the myriad of benefits that come through the use of such devices. But the applicability of RFID in other marketplaces is just beginning to be realized. One of these areas of significant potential is in medical information retrieval. The application of implantable RFID technology for medical information retrieval has been the subject of heated debate and controversy, regardless of the benefits that may be realized from such use. On one hand it has been called merely an extension of the technologies we already embrace (such as cell phones, Bluetooth devices, MP3 players, etc.), while on the other it has even been referred to as the "Mark of the Beast" by certain evangelical movements [1]. In this study, we outline some of the advantages and disadvantages of implantable RFID devices, then follow up with an in-depth survey and analysis of consumer perceptions.

Keywords: Technology Acceptance, Medical RFID, Implantable RFID.

INTRODUCTION

The pending wide-scale adoption of radio frequency identification (RFID) technologies has been the subject of significant debate in professional and academic circles for some time. Mandates by Wal-Mart, Target Corp. and Albertson's in the United States, Metro Group in Germany, and Carrefour in France have pushed the use of RFID in retailing while governmental regulations on the traceability of food in the United States and Europe have pushed RFID into food production [4]. RFID is also being used in security systems, healthcare, livestock tracking, parcel and parts tracking, casinos, U.S. toll roads, law enforcement, and the U.S. Department of Defense [2]. As the potential markets for RFID continue to expand, the inherent concerns regarding privacy risk associated with the technology become increasingly important.

RFID chips or tags are increasingly used in the healthcare industry specifically in addressing the emerging threats of diversion, theft and counterfeit medications. In addition to healthcare supply chain management, hospitals use RFID to prevent infants from being switched in nurseries and to track in-patient Alzheimer's sufferers. But while government agencies consider the use of RFID in healthcare and debate controls and regulations for the technology, privacy and consumer advocates continue to worry about the possible abuses of RFID [1][8].

In 2004, the U.S. Food and Drug Administration gave approval to VeriChip, a Florida-based company that has been developing implantable RFID chips for the past 15 years, (primarily to tag livestock and pets), to implant RFID chips in human beings for the purpose of medical information retrieval [3]. With the VeriChip system, the patient's information is not embedded upon the chip, but rather is housed within VeriChip's online, secure database. When hospital personnel pass a scanner over the implanted RFID chip, the chip's identifier is displayed on the screen of an RFID reader [5]. An authorized health professional can then use the identifier to access the patient's clinical information from the VeriChip database. Between 2004 and 2006, VeriChip claims to have implanted RFID devices in more than 2,000 people around the world, 60 of those in the United States [3].

Systems such as the VeriChip system may offer certain medical benefits, such as expedited patient identification, expedited medical records retrieval, and expedited treatment and/or problem diagnosis [5]. But such systems also raise ethical concerns regarding patient privacy.

The principal argument against RFID technology has always been and continues to be the privacy risk the technology poses to consumers. Retail items tagged with RFID chips can be scanned by anyone with an appropriate RFID scanner. According to Spiekermann and Ziekow (2005) there are five immediate and key threats posed by RFID technology, all related to the issue of privacy:

1. Unauthorized assessment of one's belongings by others
2. Tracking of persons via their objects
3. Retrieving social networks
4. Technology paternalism
5. Making people responsible for their objects

These concerns speak specifically to RFID tags found within consumer goods, but when the RFID device is within the human body, and contains a link to personal information, the issue of privacy becomes of far greater concern. Critics of the technology are particularly concerned with the risk of a patient's identifying information being used for nonmedical purposes, stating that "unauthorized access could potentially result in social discrimination, the loss of health care coverage, or the publication of potentially sensitive medical information" [5, p. 1709].

Problems with Current Implantation Standards: VeriChip

The current standard permitted by the FDA requires that no personal information be stored on an individual RFID device, but that the device contains only a unique identifier to serve as a link to a patient's medical information, housed within a separate and secure database [5]. This regulation greatly diminishes the risk of abuse of personal information related to implanted RFID devices, but does not guarantee the security or accuracy of the database containing the information. In fact, when an individual consents to implantation with a VeriChip RFID tag, he or she must sign an informed consent agreement that absolves VeriChip of any and all liability with respect to the security of its own database, as well as the accuracy of the information contained therein [8]. Even the FDA acknowledges that the VeriChip system may cause a range of technical failures and compromised information security [8].

While the VeriChip design diminishes privacy and security risk, it is not an error proof solution. VeriChip states that it does not guarantee the accuracy of the medical information stored within their secure online database [8]. It also absolves itself of any personal damage a client may incur due to a security breach, which may result in crimes such as medical ID theft [8].

In addition, hospitals are required to have special access to the VeriChip database to retrieve an individual's medical information. VeriChip's design is also proprietary, meaning that hospitals must be set up to accommodate VeriChip's design and data format. The very nature of the design demands that it be proprietary and difficult to access, otherwise the risk of unauthorized access into the system greatly increases. However, it is unlikely that all hospitals will make use of the same system, that they would agree on a standardized system of medical identification such as VeriChip, particularly as competing products are introduced to the market.

Another concern is that RFID does not fall under the protection of the Health Insurance Portability and Accountability Act (HIPAA), because it has no medical significance. Therefore there are no laws to regulate how or by whom RFID tags may be scanned, or the unique identifiers recorded. Consequently, the potential for privacy invasion and information abuse as the result of inter-database linkage is vast [5].

Alternative Design

The functionality of RFID devices is limited, and FDA regulations currently prevent increased functionality. But as the capabilities of RFID devices expand, and especially if active RFID devices (those with their own power source, capable of broadcasting their own signal) are approved by the FDA, the risk of information abuse becomes even greater, as such devices could disclose the location of the owner and/or carry significant personal information [5].

We propose that as the capabilities of RFID devices expand, particularly in regards to the amount of data the devices themselves may contain, it may be useful for consumers as well as government agencies to consider alternative means by which the technology may be used for medical information retrieval. Specifically, we are interested in evaluating consumer responses to both the VeriChip type of system, as well as another design, which would embed critical health-related information on an implanted RFID tag, but without any specific identifying information. This design would function much as the medical alert bracelets, listing significant allergies, health conditions, even organ donor information or resuscitation preferences. Such a tag could be scanned by emergency medical or hospital personnel, providing caregivers with immediate access to critical health-related information, while leaving the patient's identification to more traditional means. This design is also more accurate than the VeriChip design. Personal medical information is more likely to be correct and accurate if it is controlled by the individual, the owner of the information, rather than by a third party.

We are on the verge of massive technological advances in health care information, characterized by Google's launching of their web health services this week as well as other companies and technologies going in this direction [6]. It is imperative that we think now about the type of system we want for the future. If we can determine the types of systems consumers are more likely to accept, we can greatly increase the chances of system acceptance and thereby achieve greater efficiencies within the health care system. Health care reform continues to be a major political issue, and if reforms are forthcoming, it is important that we understand what is likely to be most acceptable to consumers.

METHODOLOGY

The research methodology was conducted using a series of semi-structured interviews conducted with both potential users of the technology as well as healthcare professionals, including paramedics, nurses, doctors and administrators. Through these interviews, we assessed the perceptions and usage intentions of potential users of the technologies, those who may suffer from the health issues these technologies address, as well as the perceptions of healthcare professionals, toward three different potential uses of implantable RFID devices for medical information retrieval.

1) The VeriChip design, which employs an implanted RFID tag containing a unique identifier that can be used to access a patient's personal medical information within a separate secure database;

2) An alternative design (CrypChip), which stores critical health-related information — such as serious allergies, permanent health conditions, etc., but no personal identifying information — directly on the RFID tag;

3) A design identical to the alternative design presented above (CrypChipPlus), but with the addition of a unique identifier (such as that employed in the VeriChip design) that can be used to link to the patient's medical record and identifying information in an online, secure database.

Interview subjects were asked to read or listen to a brief education piece outlining the basics of RFID implant technology, its benefits and liabilities, as well as a brief description of each of the three proposed design alternatives prior to offering their responses to the interview questions. They were not given additional information or encouragement, and any questions they had were left unanswered to avoid the injection of author bias. Their responses were therefore based solely on their immediate understanding of the brief presentation they received. A copy of the interview we used may be found in Appendix A.

DISCUSSION

We interviewed 13 subjects individually, five from healthcare professions and eight potential users of implantable RFID devices, to ascertain overall perceptions and preferences regarding the three alternative designs presented. Of the healthcare professionals we interviewed, three were male and two were female. Of the potential users, four males and four females were interviewed. One subject in each of the two groups refused to answer the questions completely on the grounds that they considered RFID technology to be the "Mark of the Beast," a number or identifier issued to the followers of Satan according to certain interpretations of Revelation 13:7 and 14:9-11 in the Christian New Testament.

Our healthcare professionals deemed the VeriChip design to be the least desirable and least useful of the three designs presented. It was preferred by none of the subjects and was split evenly with the CrypChipPlus design as the least secure and least trustworthy. Despite sharing the honor of least secure and least trustworthy with VeriChip, the CrypChipPlus design shared even preference with CrypChip as

well as greatest convenience benefit. The CrypChip design was unanimously preferred by those who submitted answers as the most secure design.

Regarding actual usage of the described products, four out of five of our healthcare professionals were either "not at all" likely or only "somewhat likely" to use the VeriChip design. Four out of five were also either "not at all" likely or only "somewhat likely" to use the CrypChip design. Three of the five subjects said they were "somewhat likely" or "not at all" likely to use the CrypChipPlus design. Only 26.7% of our healthcare professionals said they were "likely," "very likely" or "certain" to use any of the three described products. This is a clear indication of the reluctance of our healthcare professionals to accept implanted RFID technology. Complete results of these interviews are shown in Table 1 below.

Table 1: Results – Healthcare Professionals

Gender	Male			Female	
Profession	EMT	EMT	MD	MD	RN/Admin
Which of the three proposed systems do you prefer?	CrypChip	CrypChipPlus	CrypChipPlus	CrypChip	None
Which of the three proposed systems do you feel provides the greatest degree of personal information security for potential users?	CrypChip	CrypChip	CrypChip	CrypChip	None
Which of the three proposed systems do you feel provides the least degree of personal information security for potential users?	CrypChipPlus	VeriChip	VeriChip	CrypChipPlus	None
Which of the three proposed systems are you likely to trust most?	CrypChip	CrypChipPlus	CrypChip	CrypChip	None
Which of the three proposed systems are you likely to trust the least?	CrypChipPlus	VeriChip	VeriChip	CrypChipPlus	None
How likely would you be to use the VeriChip design?	Not at all	Not at all	Likely	Somewhat Likely	Not at all
How likely would you be to use the CrypChip design (encrypted, chip only)?	Somewhat Likely	Somewhat Likely	Certain	Somewhat Likely	Not at all
How likely would you be to use the CrypChipPlus design (encrypted, chip w/database)?	Not at all	Likely	Certain	Somewhat Likely	Not at all
Which of the three proposed systems provides the greatest convenience benefit?	CrypChip	CrypChipPlus	CrypChipPlus	CrypChip	None
Is there anything else you would like to say regarding the proposed designs that has not been addressed here?	Patient conditions change often	NA	NA	Should use for DOJ in convicts	RFID is the "Mark of the Beast"
How do you see the future of this technology?	EMTs carry too much already	NA	Very bright future	Very useful, DOJ especially	NA
What advantages and/or challenges do you see for the future of this technology?	Changes in patient conditions	NA	User resistance is a big hurdle	Turning off or shielding	NA

NA = No answer given

Like our healthcare professionals, our potential users also deemed the VeriChip design to be the least desirable and least useful of the three designs presented. It was preferred by only one of the subjects and was split evenly with the CrypChipPlus design as the least secure and least trustworthy. Despite sharing the honor of least secure and least trustworthy with VeriChip, our potential users felt the CrypChipPlus design offered the greatest convenience benefit. Meanwhile, the CrypChip design was preferred by five of the seven who submitted answers as the most secure and most trustworthy design. Interestingly, the other two subjects each chose VeriChip as the most secure. Of those two, one cited her reason for selecting VeriChip as her inability to understand the concept of data encryption, while the other indicated he chose

VeriChip because he did not understand the applicability and usefulness of a retinal scan in the other designs.

Despite their opinions regarding the usefulness of the products, however, our potential users were even less likely to use them than our healthcare professionals. Seven of eight responses issued per product were "not at all" likely or only "somewhat likely" to use. Only 12.5% of the responses issued were "likely," "very likely" or "certain." To an even greater degree than our healthcare professionals, this demonstrates a significant reluctance to accept implanted RFID technology. Complete results of these interviews are shown in Table 2 below.

Table 2: Results – Potential Users

Gender	Male				Female			
Profession	Student	Lawyer	Firefighter	Security	Childcare	Teacher	PR	Management
Which of the three proposed systems do you prefer?	VeriChip	CrypChip	CrypChip	CrypChip	CrypChipPlus	CrypChip	CrypChip	None
Which of the three proposed systems do you feel provides the greatest degree of personal information security for potential users?	VeriChip	CrypChip	CrypChip	CrypChip	VeriChip	CrypChip	CrypChip	None
Which of the three proposed systems do you feel provides the least degree of personal information security for potential users?	CrypChipPlus	VeriChip	CrypChipPlus	VeriChip	CrypChipPlus	VeriChip	CrypChipPlus	None
Which of the three proposed systems are you likely to trust most?	VeriChip	CrypChip	CrypChip	CrypChip	VeriChip	CrypChip	CrypChip	None
Which of the three proposed systems are you likely to trust the least?	CrypChipPlus	VeriChip	CrypChipPlus	VeriChip	CrypChipPlus	VeriChip	VeriChip	None
How likely would you be to use the VeriChip design?	Likely	Not at all	Not at all	Not at all	Somewhat Likely	Not at all	Not at all	Not at all
How likely would you be to use the CrypChip design (encrypted, chip only)?	Not at all	Somewhat Likely	Not at all	Somewhat Likely	Somewhat Likely	Likely	Not at all	Not at all
How likely would you be to use the CrypChipPlus design (encrypted, chip w/database)?	Somewhat Likely	Somewhat Likely	Not at all	Not at all	Likely	Somewhat Likely	Not at all	Not at all
Which of the three proposed systems provides the greatest convenience benefit?	VeriChip	CrypChipPlus	CrypChip	CrypChip	CrypChipPlus	CrypChipPlus	CrypChipPlus	None
Is there anything else you would like to say regarding the proposed designs that has not been addressed here?	Need a mandated standard	Idea of implant is unsettling	Changes in patient data problematic	Not a fan of implants	Don't get how the scans work	Safety and privacy #1 concern	NA	RFID is the "Mark of the Beast"
How do you see the future of this technology?	Not much potential	Bright, if user reluctance is overcome	Some potential	Probably significant future	Lots of potential	Huge - DOJ, DEA, Traffic control	NA	No future if we listen to the Bible
What advantages and/or challenges do you see for the future of this technology?	Too many to overcome	Accurate info and security are concerns	Changes in patient data problematic	Big Brother concerns, security	User resistance	Big Brother syndrome, too much info	NA	NA

NA = No answer given

The additional comments provided by both our healthcare professionals and our potential users offered significant insight into common concerns, other possible uses, future potential as well as possible design limitations. For example, one of our subjects expressed a concern regarding the changeable nature of a person's health. Hardcoding certain elements on the chip would therefore be counter-productive. We would not be able to record information regarding medications, temporary conditions, or other similar health-related issues on the implanted device. Doing so would require a replacement device each time a

health condition or medication changed. Encoded data must therefore be limited to critical and permanent information such as blood type, drug allergies and other permanent health conditions given the limitations of the present technology.

Privacy and security were the greatest overall concerns, particularly regarding an open source implementation. Some subjects saw so much potential for the technology in so many areas that their chief concern was the potential trafficking of too much personal information and the enormous challenges that exist in securing that much data.

One interesting concern was expressed by the EMTs we interviewed. Concerned about the amount of equipment they already carry, they felt the addition of RFID scanners would be an unnecessary encumbrance. In addition, we learned that EMTs have, through the course of their training and experience, come to rely heavily upon their ability to make quick and accurate visual diagnoses in emergency situations. They are concerned that if they were required to rely upon technology scans before administering treatment, their effectiveness, and thus the health of their patients, would be compromised. Sometimes the greatest asset is human judgement. It may be that this technology would be less applicable to EMTs and First Responders. Further research is required before any such judgement can be passed.

CONCLUSION

While we did not formulate specific hypotheses for this study, we expected to see certain results, and those results were indeed verified through this first series of interviews. First, we expected to see that people are generally reluctant to accept implanted technologies. This expectation was realized. The idea of deliberately injecting a technological device into one's body is not necessarily appealing, and is considered by most people to be invasive. A significant convenience benefit must be demonstrated before such reluctance can begin to be alleviated.

Second, we expected our subjects' most prevalent concerns to be the privacy and security of their personal and private information. This expectation was realized. A significant convenience benefit, coupled with high-confidence security measures must be demonstrated before such reluctance can begin to be alleviated. However, our subjects' resistance to both the VeriChip and CrypChipPlus designs, designs that incorporate online databases, demonstrates additional concerns regarding both the security *and the accuracy* of the data. Where a third party is involved in maintaining medical records, data accuracy becomes a key issue. Further research is required to develop sound data integrity control mechanisms before consumer confidence can begin to improve in this area.

Third, we expected to see concerns regarding the implementation of open source software for the purpose of decrypting the data stored on the RFID device, as well as for the proposed medical records database suggested with the CrypChipPlus design. This expectation was also realized. Significant security measures must be researched and developed to ensure the protection and integrity of the recorded personal information in an open source environment.

Finally, we expected to encounter a level of resistance from those who oppose RFID technology in all its forms for religious reasons. This expectation was also realized. Two of our thirteen respondents, one from each of the two categories, both female, refused to answer the questions completely on the basis that they believed RFID to be the "Mark of the Beast" as spoken of in the book of Revelation in the Christian Bible. While many consider the association of the "Mark of the Beast" with RFID technology to test credulity at best, it is a public perception that cannot be ignored. Books such as *Steps Toward the Mark of the Beast* by Glenn A. Guest and, most notably, *Spychips: How Major Corporations and Government Plan to Track Your Every Move with RFID* by Katherine Albrecht and Liz McIntyre have been rather

successful at vilifying RFID technology through misrepresentation and gross inaccuracies regarding the capabilities and potential uses of the technology. This perception of RFID may not be a predominant perception, but it is popular enough to render significant resistance to the adoption or acceptance of the technology, particularly regarding implantable RFID devices, regardless of any verifiable benefit. This may be one of the most difficult challenges RFID technology faces. Religious zeal if a powerful force that is not easily dissuaded. Despite attempts by many theologians and clergymen to discredit the misguided notions presented by authors such as Albrecht, McIntyre and Guest through counter publications and sermons, religious opposition to RFID continues to grow. Further research is necessary to determine whether education can alleviate concerns of this nature. A study involving active as opposed to passive RFID tags, perhaps where the active tags can only be "turned on" or activated by authorized healthcare personnel, may see a reduction in the "Mark of the Beast" comparisons.

Despite their personal resistance to the technology, most of our respondents believe in a significant future for RFID devices, implanted and otherwise. Subjects suggested it be used for Department of Justice applications, specifically for the tagging and tracking of convicts and parolees, especially sexual predators. Other suggested uses were for drug enforcement applications and traffic control, especially unmanned speed monitoring. We are only beginning to realize the potential of this technology, but it will require significant future research to determine whether consumers are willing to accept that potential.

REFERENCES

[1] Albrecht, K. and McIntyre, L. (2005) *Spychips: How Major Corporations and Government Plan to Track Your Every Move with RFID*, Thomas Nelson (October 4, 2005).

[2] Attaran, M. (2006), "RFID pays off ", *Industrial Engineer*, Vol. 38, No. 9, pp. 46.

[3] Bahney, A. (2006), "High Tech, Under the Skin", *New York Times*, Feb. 2, 2006.

[4] Dave, D. S., Cazier, J. A. and Jensen, A. S. (2007), "The Impact of Residual RFID Logistics on Consumer Use and Purchase Intentions", presented at the *43rd Annual Meeting of Southeastern Chapter of INFORMS*, Myrtle Beach, South Carolina, USA, October 1, 2007.

[5] Levine, M., Adida, B., Mandl, K., Kohane, I. and Halamka, J. (2007), "What Are the Benefits and Risks of Fitting Patients with Radiofrequency Identification Devices?" *PLoS Medicine*, Vol. 4, No. 11, pp. 1709-1711.

[6] Needleman, R. (2008), "Google Health: Great idea, but scary as all get out", *CNET Networks, Inc.*, May 18, 2008, < http://www.webware.com/8301-1_109-9947826-2.html?tag=nl.e776>, May 25, 2008.

[7] Spiekermann S. and Ziekow H. (2005), "RFID: A 7-Point Plan to Ensure Privacy" In Proceedings of the *Thirteenth European Conference on Information Systems* (Bartmann D, Rajola F, Kallinikos J, Avison D, Winter R, Ein-Dor P, Becker J, Bodendorf F, Weinhardt C eds.), Regensburg, Germany.

[8] Wolinsky, H. (2006), "Tagging Products and People", *EMBO Reports*, Vol. 7, No. 10, pp. 965-968.

APPENDIX A – Interview: Implanted RFID Devices for Medical Information Retrieval

RFID Medical Implants - Introduction

In 2004, the FDA approved the use of implanted RFID technology in humans. RFID implants are very small Radio Frequency Identification (RFID) devices, about the size of a grain of rice, that can be implanted virtually anywhere on the body, but are often inserted into the soft tissue between the thumb and forefinger. These devices hold a very small amount of data, typically just a 15-digit alpha-numeric code that is used to uniquely identify the device and the person or object associated with it. RFID implants have been used for a variety of purposes, from VIP treatment in European nightclubs to linking implantees to their medical records in an online database.

Medical information retrieval is a usage area for this technology that shows significant promise, but that has also received equally significant criticism. Critics of the technology are particularly concerned with the risk of a patient's identifying information being used for nonmedical purposes, stating that "unauthorized access could potentially result in social discrimination, the loss of health care coverage, or the publication of potentially sensitive medical information." There are certain benefits, however, such as rapid condition identification and treatment, particularly regarding emergency care, that such devices offer to both healthcare providers and patients. This survey explores three alternative designs for such devices and seeks patient and healthcare provider feedback regarding these designs.

Possible Implant Alternatives

1. VeriChip — the patient's information is not embedded upon the chip, but rather is housed within VeriChip's online, secure database. When hospital personnel pass a scanner over the implanted RFID chip, the chip's identifier is displayed on the screen of an RFID reader. An authorized health professional can then use the identifier to access the patient's clinical information from the VeriChip database.

Pros	Cons
Personal medical and identifying information is stored in a secure, online, third-party database.	Requires users to sign informed consent absolving VeriChip of liability pertaining to the security as well as accuracy of personal data.
Only VeriChip authorized hospitals, clinics, and medical personnel can access medical records.	Proprietary – requires hospitals to set up VeriChip accounts and to have special access to VeriChip databases to retrieve medical information.
Relatively inexpensive for consumers – about $400 per chip + $10 - $80 annual fee for information storage (depending on plan) – and for most hospitals, scanners are about $600.	Widespread effectiveness requires all hospitals and care centers to use the same system.
Users can choose among different storage plans – from minimal information such as contact and doctor info to complete medical histories and records.	May be cost-prohibitive to smaller or rural hospitals and clinics, as well as low-income patients.

2. CrypChip — stores critical health-related information — such as serious allergies, health conditions, etc., but no personal identifying information — directly on the RFID tag; this data is encrypted to protect the privacy of the individual, using an encryption key that is based upon a unique biometric feature, such as a retinal scan.

Pros	Cons
No identifying information	No identifying information – identification must be done through more traditional means
Open source, free software, no contracts or proprietary software required – available and usable by virtually all clinics, hospitals, emergency personnel.	
Encrypted data, with encryption key tied to unique biometric feature (retinal scan)	Retinal scan can be prone to false rejection, other biometric features have potential drawbacks

3. CrypChipPlus — identical to CrypChip, but with the addition of a unique identifier (such as that employed in the VeriChip design) that can be used to link to the patient's complete medical record and identifying information in an online, secure database.

Pros	Cons
No identifying information on chip	Database must be managed by third party at additional cost.
Chip includes link to medical record in online, secure open-source database	Accuracy and security of database records cannot be guaranteed.
Open source, free software, no contracts or proprietary software required, inexpensive hardware – scanner	
Encrypted data, with encryption key tied to unique biometric feature (retinal scan)	Retinal scan can be prone to false rejection, other biometric features have potential drawbacks

RFID Medical Implants – Questions

1. Which of the three proposed systems do you prefer, and why?
    a. As a patient?
    b. As a healthcare provider?

2. Which of the three proposed systems do you feel provides the greatest degree of personal information security for potential users, and why? The least?

3. Which of the three proposed systems are you likely to trust most? The least?
    a. As a patient?
    b. As a healthcare provider?

4. As a healthcare provider, how likely would you be to use the VeriChip design?

    Not at all Somewhat Likely Likely Very Likely Certain

As a patient?

Not at all *Somewhat Likely* *Likely* *Very Likely* *Certain*

5. As a healthcare provider, how likely would you be to use the CrypChip design (encrypted, chip only)?

   Not at all *Somewhat Likely* *Likely* *Very Likely* *Certain*

   As a patient?

   Not at all *Somewhat Likely* *Likely* *Very Likely* *Certain*

6. As a healthcare provider, how likely would you be to use the CrypChipPlus design (encrypted, chip w/database)?

   Not at all *Somewhat Likely* *Likely* *Very Likely* *Certain*

   As a patient?

   Not at all *Somewhat Likely* *Likely* *Very Likely* *Certain*

7. Which of the three proposed systems provides the greatest convenience benefit for healthcare providers? For patients?

8. Is there anything else you would like to say regarding the proposed designs that has not been addressed here?

9. How do you see the future of this technology?

10. What advantages and/or challenges do you see for the future of this technology?