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

***Andrew S. Jensen***
Department of Computer Science
College of Computing and Informatics
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 a discussion and analysis of consumer perceptions gained from a series of semi-structured interviews with potential users and healthcare professionals, including paramedics and firemen, nurses, doctors and administrators.

**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, regular medications, 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 propose that the data contained on the chip be coded in a series of bits indicating a positive or negative flag for several common medical conditions, from allergies to Penicillin or bee stings to cardiac conditions and diabetes. To protect the individual's data from unwarranted scanning, we propose the data be encrypted using an encryption algorithm whose decryption key would be tied directly to a biometric feature unique to the individual, such as a retinal scan. The encoded data could therefore be decrypted whether the individual was conscious or not. A simple, open-source software program can be written to initiate and process the decryption of the data stored in the implanted RFID tag upon completion of the appropriate biometric scan, providing emergency caregivers with immediate critical information regarding the individual's specific health needs.

Using an open-source software solution for this system renders this an inexpensive and easily-implemented solution for healthcare facilities, as opposed to the proprietary and exclusive contracts that would be required by other, more elaborate solutions. Such a benefit would make this solution more attractive to lower budget facilities, such as hospitals and emergency clinics in rural areas.

We are on the verge of massive technological advances in health care information, characterized by Google's recent launching of their web health services 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 will be conducted using a series of semi-structured interviews conducted with both potential users of the technology as well as healthcare professionals, including paramedics and firemen, nurses, doctors and administrators. Through these interviews, we will assess 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 four 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, which stores critical health-related information — such as serious allergies, required medications, health conditions, etc., but no personal identifying information — directly on the RFID tag;

3) A design identical to the alternative design presented above, but with the added security of data encryption, with the encryption key tied to a unique biometric feature, such as a retinal scan.

4) A design identical to the alternative design presented above, 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.

Interview subjects will be asked to listen to a brief education piece outlining the basics of RFID technology, its benefits and liabilities, as well as a brief but detailed description of each of the four proposed design alternatives prior to offering their responses to the interview questions. Results of the study will then be analyzed and a discussion of the results will be presented at the conference.

## 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.