International Journal of Technology Assessment in Health Care, **26:4** (2010), 370–376.

doi:10.1017/S0266462310001133

Implanting inequality: Empirical evidence of social and ethical risks of implantable radio-frequency identification (RFID) devices

Torin Monahan, Jill A. Fisher
Vanderbilt University

Objectives: The aim of this study was to assess empirically the social and ethical risks associated with implantable radio-frequency identification (RFID) devices.
Methods: Qualitative research included observational studies in twenty-three U.S. hospitals that have implemented new patient identification systems and eighty semi-structured interviews about the social and ethical implications of new patient identification systems, including RFID implants.
Results: The study identified three primary social and ethical risks associated with RFID implants: (i) unfair prioritization of patients based on their participation in the system, (ii) diminished trust of patients by care providers, and (iii) endangerment of patients who misunderstand the capabilities of the systems.
Conclusions: RFID implants may aggravate inequalities in access to care without any clear health benefits. This research underscores the importance of critically evaluating new healthcare technologies from the perspective of both normative ethics and empirical ethics.

Keywords: Ethics, Patient identification systems, ICT implants, Technology, Privacy

Implantable radio-frequency identification devices (RFID implants) for patient identification are said to have the potential to increase accuracy of identification and streamline healthcare delivery, but they may also introduce new medical, social, and ethical risks. To date, concerns about implants have been largely hypothetical, focusing on the safety of the devices, privacy of patients' records, and coercion to consent to the implantation of the devices. While these risks to patients are important to attend to, this article reports the results of an empirical study to show that there are additional risks associated with these new technologies that arise from their use in the context of healthcare delivery. These findings underscore the importance of studying technologies in their social context.

BACKGROUND

The U.S. Food and Drug Administration approved RFID implants for human use in 2004 (18). The system requires the insertion of a small, glass-encased microchip into the triceps region of patients' arms. After implantation, medical staff or others can scan the chip with a hand-held reader to reveal a unique identifying number. Staff can then use this number to access patients' health records from an online database

called VeriMed, run by the VeriChip Corporation (recently renamed "Health Link") (22). The rationale for the system is to help hospital staff properly identify patients who might be unable to communicate. The company asserts that RFID implants can give healthcare personnel access to a patient's name, medical history, allergies, and advance directives so that rapid and appropriate treatment can be provided (18). According to one report, 900 hospitals have agreed to participate in the VeriMed system, 600 people have received RFID implants to date, and the company has begun direct-to-consumer advertising campaigns in targeted markets, such as South Florida, to increase this number (22).

While the major deployment of RFID implants in health care has been in the United States, the European Commission has been following the development of RFID technologies more generally and proposing guidelines to govern their uses. That the United States is the major focus of VeriChip's marketing of the implant should come as no surprise. In a country with an extremely fragmented healthcare delivery system, personal health records (PHRs), like VeriMed, are increasingly touted as the best solution for patients to have centralized access to their medical records (23). The majority of organizations offering PHRs are commercial companies that offer subscriptions for a repository in which patients can keep their medical information, but the burden is usually on patients to populate their records themselves. In the European context, questions about the ethical use of implants (often referred to as "ICT implants") have received focused attention by scholars, as evinced by an international workshop on the topic held at The Center for Interdisciplinary Research at Bielefeld University in Germany in 2008. Interest in RFID implants in Europe also extends beyond medical applications to include entertainment and commercial functions, such as the Baja Beach Club in Barcelona, Spain, which allows patrons to keep an electronic bar tab through a subdermal implant system (17). What is unique about the attention given to implants in the United States and internationally is that unlike most emergent technologies, they are perceived as a fraught device, with negative potentialities that must be discussed before widespread adoption.

Although there is a dearth of literature on RFID implants, scholarly attention to these devices has primarily come from the fields of bioethics and information ethics and from privacy advocates. With few exceptions, ethicists set their sights foremost on the potential of implants to create health risks, threaten individual privacy, and to be used coercively (6;7;21). First, the most direct concern with RFID implants is that they might pose health risks to patients, such as emitting radio waves that could cause tumors, migrating throughout one's body, or requiring surgery to have them removed. Foster and Jaeger (6) write, for instance, about the need to inform patients about findings indicating carcinogenic effects of RFID implants in rodents. Furthermore, because other RFID systems have been shown to induce electromagnetic interference in medical devices (24), the introduction of RFID implants and their related scanning systems in hospitals could potentially cause serious medical complications and endanger patients.

Without question, loss of privacy is the main concern that ethicists and others have about RFID implants (4;6;13). As with the use of RFID chips embedded in identity documents, such as passports, the threat is that information will be "read" surreptitiously by government agents, corporate entities, or malicious others, such as identity thieves, and that confidential and/or sensitive data will be obtained or shared without one's knowledge (14). In the context of what has been referred to as "the surveillance society" (15), RFID devices add one more layer of technologies that create, store, and circulate information about people, their habits, histories, predispositions, and preferences. As Glasser et al. (9) relate: "Perhaps the greatest concern with tracking humans [with RFID implants] is that it may lead to increased and even ubiquitous spying, surveillance and stalking" (p. 106). Although the discourse of privacy is both an important and expected response to new systems of identification and monitoring, other scholars have noted that privacy may be an insufficient concept in that it tends to focus attention on individuals, not groups, and it does not adequately allow for a critique of unequal power relations (8).

A third problem identified with RFID implants is the risk of coercion. Simply put, ethicists, privacy advocates, and others worry that someday people may be "chipped" without consent, perhaps as part of a mandated government program to monitor and regulate the movement of people within a county's borders (1;6). Indeed the implementation of a program to chip employees at a U.S. security company, *with* their consent, prompted legislation in several U.S. states to prohibit the involuntary chipping of anyone (16;18). In sensationalist terms, some scholars write: "What person would ever choose to have such a device implanted? Perhaps people will not have a choice. Parents may choose to have such a unit implanted in their child at birth. . . If those who are incapable of consent begin to be injected with an identification microchip, privacy advocates certainly should raise an alarm" (14). The general conclusion, then, is that legislation is necessary to prevent dystopian science-fiction scenarios from becoming reality (9;12;14). Given that the patient population currently most heavily recruited to receive RFID implants is geriatric patients, especially those with Alzheimer's disease or dementia (19), concerns about receiving informed consent are not merely theoretical.

These three concerns (health risks, threats to individual privacy, and coercion) guide most critical discussions of RFID implants. What they tend to neglect, however, is attention to the specific contexts within which such systems are deployed. They also tend to be based on speculation about technological futures rather than grounded in present empirical realities. Because economic and other inequalities characterize the current U.S. healthcare system and shape technology use, one should expect that inequalities would

inflect the deployment of RFID implants too. An empirical examination of RFID implants in healthcare contexts, where they stand the greatest chance of being adopted in the short term, indicates that these devices portend a host of other problems that we argue should be construed as ethical in nature. Namely, RFID implants threaten to reify social inequalities, attenuate trust relationships among patients and medical staff, and even endanger patients. In the sections that follow, we provide a brief overview of our study and then turn to examples of risks the devices pose in hospital settings.

METHODS

The data presented here are part of a larger national study of identification and location systems in U.S. hospitals, which was conducted by the authors between March 2007 and December 2009. The primary aim of the research was to investigate the social and ethical concerns that are associated with these new hospital technologies. RFID implants are one such technology included in our study. The research questions were as follows: (i) What effects do RFID systems have upon organizational roles and relations?, and (ii) What are the surveillance potentials of RFID systems? The focus of these questions included documentable practices and policies as well as hospital staff's perceptions of the changes brought about by the RFID systems.

The methods for the project involved site visits to hospitals that had implemented systems to identify or track patients, staff, and/or equipment. During site visits, we observed the systems in use and conducted semistructured interviews with personnel. The project included twenty-three U.S. hospitals that were selected based on their use of a qualifying system (as identified through personal contacts, press releases, or media coverage) and their receptivity to participating in the research. The majority of the hospitals were in the eastern part of the country, with five in New England, nine in the Mid-Atlantic, and six in the Southeast. Two hospitals were located in the Midwest, and one was in the West. Demonstrations of the systems ranged from formal presentations made by personnel in charge of the system to informal observations of users interacting with the system. These demonstrations provided first-hand evidence of—and, therefore, offered critical insights into—the capabilities and usability of the systems. It should be noted that even when demonstrations were clearly staged for our benefit, the flaws of the systems were usually evident. In some cases, this was because the systems did not work as promised. One particularly common manifestation of this was that a selected item could not be tracked and located. In other cases, the interfaces were so cumbersome that the user struggled with the demonstration. This type of problem tended to occur when one of us would ask a question about the system, and the user would attempt (usually unsuccessfully) to run a report or to show an alternative view of the data about which we had asked. In other words, the observations of the systems gave insights into both the functions and the flaws of the systems, including users' facility with those systems.

In addition to informal conversations held while observing the systems, we conducted 80 semistructured interviews. Sixty-seven interviews were conducted with hospital staff, including twelve physicians (eleven men, one woman), six nurses (all women), twenty-one administrators (ten men, eleven women), twelve information technology specialists (eight men, four women), seven biomedical engineers (six men, one woman), and nine clerical staff (six men, three women). These counts are based on interviewees' predominant role in the hospital, but some administrators were also non-practicing physicians and nurses, which clearly influenced their professional identities if not their job descriptions. Interviewees were recruited from hospital employees who make decisions about or are targeted users of the systems. While the average number of interviews per hospital was three staff members, the actual range was much wider, varying from one employee at several hospitals to as many as eleven at one hospital site. The number of interviews per hospital was dependent primarily on the number and type of staff involved with the systems, which varied considerably across the hospital sites. An additional twelve interviews were conducted with vendors (ten men, two women) from seven companies that were working with these hospitals to install or maintain the systems under investigation. The number of vendors selling these types of hospital technologies is limited, so the companies represented in our study were working with multiple hospitals where we conducted site visits. Finally, although the focus was on the use of the systems by hospital employees, patients were included in our observations at hospitals and one formal interview was conducted with a white, male patient. The identities of hospital sites and all interviewees were given confidentiality in the study, and all participants provided informed consent.

We then analyzed all interview transcripts and observational notes to identify core themes, such as key ethical concerns associated with these systems. Coding was multistaged, so that the data were revisited multiple times for depth of analysis and for the creation of cross-references among the data and the categories coded. The process of coding was done by discussing the data together at the conclusion of site visits and by individually adding to the coding through the process of a fine-grained reading of transcripts and observational notes for additional themes that emerged as important. Initial coding was limited to broad categories as defined by the following pre-defined core variables and organizing themes: (i) Management goals and orientation, (ii) Organization of labor, (iii) Distribution of material resources, (iv) Formal and informal policies regarding surveillance of individuals or groups, and (v) Attitudes and perceptions of staff. For example, we examined the discourse mobilized by administrators about the goals they set for the RFID systems.

We queried who was given authority in decision making about the systems and who was responsible for carrying out the daily tasks needed to make the systems work. We coded for issues surrounding division of labor, looking at which staff were involved and the ways in which the systems translated into increases or decreases in labor for those staff. We were attentive to the material and financial constraints that each hospital had as well as territoriality within hospitals, which often played into the distribution of resources. As part of our interest in the surveillance potential of these technologies, we coded the presence and absence of policies—both formal and informal—guiding the use of the systems, and we coded the ways that surveillance of employees was allowed to occur and the practices that minimized this type of activity. Other variables included hospital staff's attitudes about and perceptions of the systems in their hospitals. These data were drawn from semistructured interviews, observation of staff's conversations with each other and with patients, and informal conversations directly with hospital staff. During later coding, we added more subtle codes, such as those relating to issues of organizational dynamics like those influenced by gender and power. One important theme that we found emerged from a particular RFID technology, subdermal implants, which is the focus of the discussion in this paper.

RESULTS

Scholars have called attention to the threats to privacy, informed consent, and patient health due to complications with RFID implants. Our empirical research has found an additional set of social and ethical risks associated with this technology. Our findings include three themes that emerged from our analysis regarding potential risks of implants: (i) unfair prioritization of patients, especially in triage; (ii) diminished trust of patients; and (iii) endangerment of patients.

Unfair Prioritization of Patients

The decision to receive an RFID implant is not simply a matter of willingness but more significantly a question of having the means to pay monthly subscription fees. The consumer model for the implant system is not to be underestimated because our findings indicate that it privileges those with more resources and disadvantages those with fewer. Most patients electing to receive an implant and enroll in the system must pay both for the cost associated with being implanted, estimated at $200 to $300, and a monthly fee of $9.95 with a minimum of a 2-year contract (25). This effectively excludes many patients who cannot afford the fees associated with the system.

More importantly, this model may prove coercive as well: it can compel patients to get implants by promising them better (or more prompt) care in exchange. One physician whom we interviewed advocated for this consumer model with regard to RFID implants. He told us,

> I think that. . . a lot of people will see the benefit [of implants] and go for it, especially if they're in a healthcare situation and the person that has the chip gets scanned and moves along with their workup and the other person's [still] waiting to have their blood drawn.

Providing expedited care to patients who have implants is certainly one way of encouraging the technology's adoption, but as with "concierge" medicine (2;20), it privileges those who can pay out-of-pocket for non-essential healthcare services.

Diminished Trust of Patients

Healthcare providers indicated that they would be more likely to trust the information contained in the VeriMed system than information gleaned from patients themselves. An excerpt from an interview with a provider at a large hospital that is using the VeriMed system illustrates this point:

> *Interviewer*: *What would you do if a patient was telling you one thing and the chip was saying something else?*
>
> Informant: I'd probably say the patient was disoriented at the time, probably didn't really know what he was talking about. So we just go based on the chip because that's probably the most accurate information we can get.
>
> *Interviewer*: *Even if it's something as basic as his name?*
>
> Informant: Well I think, I mean we have patients that come in that give us false names, false insurance cards, so that's why it depends.

Although patients might indeed lie about their identities, it should cause concern that a healthcare provider believes that the commercial VeriMed system would provide the "most accurate information" about a patient. Within this framework, the absence of documentation in the VeriMed health record can be interpreted incorrectly as patients' absence of allergies, existing medical conditions, prior surgeries, medications, and so forth. Any of these can be dangerous assumptions in the treatment of patients. In other words, provider trust in the technology creates the potential for serious medical errors.

Endangerment of Patients

Another significant problem with RFID implants that we identified is the risk of endangering patients as a result of poor or lax informed consent processes. For example, during one session of participant observation at a hospital that is actively "chipping" patients with RFID implants, we witnessed a troubling encounter between a physician and patient in his 90s, who received an implant. When we asked the patient why he wanted the device, he launched into a frightening story about collapsing in his home four months earlier. He had difficulty signaling for help because he kept passing out.

https://doi.org/10.1017/S0266462310001133 Published online by Cambridge University Press

What was especially disturbing about the patient's response to our question was that he appeared to believe that the implanted RFID would assist emergency personnel in knowing whether he collapsed again and in finding and treating him promptly if he did. As a result, he may, in fact, be much more in danger *with* the implant than without it because he believes it can do things that it cannot (i.e., monitor his vitals and send signals for help and locational information if needed). The physician who was implanting the patient was in the room during this exchange and seemed anxious to continue with the procedure. He did not correct the patient about his misunderstanding of the functionality of the technology or its purpose. In fact, the physician was decidedly annoyed when one of us tried to inform the patient. Rather than intervening himself, the physician pushed a series of "releases" over to the patient for his signature, which he never explained and which the patient did not read before signing.

Cases like this one indicate the extent to which patients are not fully informed about RFID implants and the dangers associated with a misunderstanding about the technology. This encounter also underscores the extent to which some physicians are not taking seriously their responsibility to inform their patients about the *functions*, let alone the risks, of implants. Given that we were present during this doctor–patient encounter and that the physician did not attempt to inform the patient despite the clear need to do so, we can surmise that ethical issues with the chipping of patients are not even on the radar screens of many physicians.

DISCUSSION

These findings reveal a mismatch between previously documented scholarly concerns with RFID implants and their actual uses. While we are entirely sympathetic to and in agreement with most of the recommendations made by bioethicists, information ethicists, and privacy advocates about these devices, they are not grounded in the empirical realities of U.S. hospitals. Attention to mundane, everyday uses of these systems in particular organizational contexts can draw attention to a range of basic, somewhat predictable—but nonetheless serious—risks engendered by the VeriMed system.

U.S. hospitals are grounded in political and economic contexts that are marked by inequality in access to care (10). Part of that context is an entrepreneurial ethos circulating in the healthcare system, which encourages physicians, hospital administrators, and others to be at the forefront of technological change, or what is sometimes referred to as the "bleeding edge" of technological advancement (11). These contextual factors shape the ways in which RFID implants are being used and interpreted. These factors likewise shape the attendant social and ethical risks RFID implants pose to patient populations.

One ethical concern regarding RFID implants is their potential to *exacerbate* existing inequalities in access to care. Physicians perceive implants as a device that will lead to differential access to healthcare. Similar to preferred shopper programs or airport priority programs that allow people to have better or expedited access to particular services, RFID implants could serve a similar function of granting chipped patients speedier access through triage or other healthcare interactions. Technologies like these can lead to "social sorting" in which people are treated differently based on their social position and access to technology (15). As they are being used now, RFID implants have a propensity to prioritize patients who can afford to subscribe to the VeriMed system.

The second ethical issue we identified is that RFID implants are linked to one more informational database that can be seen as more accurate than a patient's words. Diminished trust in patients, and increased trust in various technological databases, monitors, and instruments, is nothing new in the history of technological innovation in health care (10). What should give us concern, however, is the combination of this faith in technology with the potential unreliability of patients' records. Commercial personal health record systems, like the one associated with RFID implants, rely in large part on user input of data and are not likely to be robust, but, as our research found, providers do not perceive this deficiency in the system.

The third ethical concern discovered in our empirical research relates to the potential endangerment of patients that can accompany RFID implants. Whereas the typical concern flagged in the literature is that people will be chipped involuntarily, we found that some patients get chipped without adequate knowledge of how the system works. The populations who are considered prime candidates for implants are the most likely to have difficulty giving informed consent (6). This is true not only because many patients are elderly but also because of inadequate consent procedures. It is also important to note that as with many other informed consent procedures, the spatial setting of a professional healthcare context conveys to patients messages of medical authority that encourage them to trust medical professionals and to downplay risks indicated on consent forms (5). In our research, we have found that patients have considerable misunderstanding about the technological capabilities of the implants for their health and safety. More troubling is that physicians may not be correcting these misunderstandings before they implant RFID chips in patients. This is of grave concern, because it might place patients at greater risk in a medical emergency.

Our study does have several limitations. First, because we were not setting out to do an in-depth empirical study of RFID implants, this technology was just one type among many systems that were included in our research. A more focused study of RFID implants that followed patients who received the device would be better able to address the extent

to which patients' understanding of the technology changes over time and how well they are able to use the personal health record interface. Second, we studied only the U.S. context, which is considerably different than other industrialized countries, so it is difficult to know if the concerns we identify here would apply equally in other countries. Nonetheless, given the current dearth of empirical information about RFID implants, our findings are an important first step in understanding the social and ethical risks associated with this new technology.

CONCLUSIONS

RFID implants are a futuristic-sounding technology, the likes of which have elicited concerns about bodily harm, loss of privacy, and involuntary chipping. The responses given by bioethicists, information ethicists, and privacy advocates to these particular concerns focus on the need to invoke some version of the precautionary principle (3) and to enact legislation to prevent the technology from being used without full transparency and informed consent (14). Depending on how they are used, however, they may also aggravate inequalities in access to care, diminish trust in patients, and introduce new health risks.

Moreover, it is quite unclear what health benefits RFID implants offer that are significantly better than other technologies or systems that help identify patients and provide critical health information. This research underscores the importance of critically evaluating new healthcare technologies from the perspective of both normative ethics and empirical ethics. By unpacking and challenging the market logics driving RFID implants and their healthcare applications, the development of new technological systems, such as this one, stand a better chance of being redirected toward more equitable and ethical healthcare provision.

ACKNOWLEDGMENTS

This material is based upon work supported by the U.S. National Science Foundation under grant numbers SES-0642797 and SES-0907993.

CONTACT INFORMATION

Torin Monahan, PhD (torin.monahan@vanderbilt.edu), Associate Professor, Department of Human & Organizational Development, Department of Medicine, Vanderbilt University, Peabody #90, 230 Appleton Place, Nashville, Tennessee 37203-5721

Jill A. Fisher, PhD (jill.fisher@vanderbilt.edu), Assistant Professor, Center for Biomedical Ethics & Society, Vanderbilt University, 2525 West End Avenue, Suite 400, Nashville, Tennessee 37203

CONFLICT OF INTEREST

T. Monahan and J. Fisher have received grants from the U.S. National Science Foundation for this work.

REFERENCES

1. Albrecht K, McIntyre L. *The spychips threat: Why Christians should resist RFID and electronic surveillance*. Nashville, TN: Nelson Current; 2006.
2. Borfitz D. Make your practice more profitable. *Med Econ.* 2001;78:106, 109-110, 114-116.
3. Clarke S. Future technologies, dystopic futures and the precautionary principle. *Ethics Inf Technol.* 2005;7:121-126.
4. Crooker K, Baldwin D, Chalasani S. RFID technology as sustaining or disruptive innovation: Applications in the healthcare industry. *Eur J Sci Res.* 2009;37:160-178.
5. Fisher JA. Procedural misconceptions and informed consent: Insights from empirical research on the clinical trials industry. *Kennedy Inst Ethics J.* 2006;16:251-268.
6. Foster KR, Jaeger J. Ethical implications of implantable radiofrequency identification (RFID) tags in humans. *Am J Bioeth.* 2008;8:44-48.
7. Gadzheva M. Getting chipped: To ban or not to ban. *Inf Commun Technol Law*. 2007;16:217-231.
8. Gilliom J. *Overseers of the poor: Surveillance, resistance, and the limits of privacy*. Chicago: University of Chicago Press; 2001.
9. Glasser DJ, Goodman KW, Einspruch NG. Chips, tags, scanners: Ethical challenges for radio frequency identification. *Ethics Inf Technol.* 2007;9:101-109.
10. Gray BH. *The profit motive and patient care: The changing accountability of doctors and hospitals*. Cambridge: Harvard University Press; 1993.
11. Kleinke JD. *Bleeding edge: The business of health care in the new century*. Gaithersburg, MD: Aspen Publishers; 1998.
12. Laurant C, Farrall K. RFID Workshop Comment P049106. FTC Workshop on Radio Frequency Identification: Applications and Implications for Consumers. 2004.
13. Levine M, Adida B, Mandl K, Kohane I, Halamka J. What are the benefits and risks of fitting patients with radiofrequency identification devices. *PLoS Med.* 2007;4:1709-1711.
14. Lockton V, Rosenberg RS. RFID: The next serious threat to privacy. *Ethics Inf Technol.* 2005;7:221-231.
15. Lyon D. *Surveillance studies: An overview*. Cambridge: Polity Press; 2007.
16. Michael K, Michael MG. Predicting the socioethical implications of implanting people with microchips. *PerAda Magazine*. 2009. http://www.perada-magazine.eu/view.php?article = 1598-2009-04-02 (accessed September 1, 2010).
17. Michael K, Michael MG. The diffusion of RFID implants for access control and ePayments: Case study on Baja Beach club in Barcelona. *Proc IEEE Int Symp Technol Soc (ISTAS10)*. 2010:242-252.
18. Monahan T, Wall T. Somatic surveillance: Corporeal control through information networks. *Surveill Soc.* 2007;4:154-173.
19. Niemeijer A, Hertogh C. Implantable tags: Don't close the door for aunt millie! *Am J Bioeth.* 2008;8:50-52.

20. Pham HH, Devers KJ, May JH, Berenson R. Financial pressures spur physician entrepreneurialism. *Health Aff (Millwood)*. 2004;23:70-81.
21. Sade RM. *Report of the Council on Ethical and Judicial Affairs: Radio frequency ID devices in humans*. Chicago: American Medical Association; 2007.
22. Swedberg C. VeriChip markets its implantable RFID tags and services direct to consumers. *RFID Journal*. 2008.
23. Tang PC, Ash JS, Bates DW, Overhage JM, Sands DZ. Personal health records: Definitions, benefits, and strategies for overcoming barriers to adoption. *J Am Med Inf Assoc*. 2006;13:121-126.
24. Van Der Togt R, van Lieshout EJ, Hensbroek R, et al. Electromagnetic interference from radio frequency identification inducing potentially hazardous incidents in critical care medical equipment. *JAMA*. 2008;299:2884-2890.
25. VeriMed. *Intro to VeriMed: FAQ*. 2008. http://www.verimedinfo.com/faq.asp (accessed March 14, 2009).