Radio Frequency Identification in Hospitals: Balancing Hospital Efficiency and Patient Privacy

Christopher A. Suarez
Yale Law School, USA

This paper will appear in PERSONAL DATA PRIVACY AND PROTECTION IN A SURVEILLANCE ERA: TECHNOLOGIES AND PRACTICES, edited by Christina Akrivopoulou and Athanasios Psygkas, Copyright 2010, IGI Global. Posted by permission of the publisher.

Abstract

Radio Frequency Identification technology has increasingly been applied within the hospital setting for various purposes. This paper argues that, while such applications may drastically improve hospital efficiency, they also may produce privacy risks that harm patients more than they help them. Further, the privacy risks associated with such technologies are difficult to comprehend. When patients' personal data is implicated, hospitals should adhere to privacy principles that promote the flow of full information and enable patients to make rational choices when they opt-in to hospital RFID applications. Otherwise, RFID hospital technologies may be implemented in ways that do not serve patients' long term privacy interests.

Introduction

Although radio frequency identification (RFID) has been in existence for over 50 years, it was not recommended for use in many applications until recently because it is still relatively expensive and underdeveloped. As consultants and investors saw the potential moneymaking opportunities that could arise from RFID, however, there has been a substantial push for its continued development. Starting with Wal-Mart's 2004 mandate to its Top 100 suppliers requiring them to use RFID in their supply chains, a huge buzz was created that envisioned all sorts of RFID applications (Fanberg 2004). Meanwhile, consumer privacy advocates rolled up their sleeves, pointing out a myriad of privacy concerns posed by particular applications of RFID. They asserted that, while RFID is a technology that can produce tangible benefits, the negative privacy implications of RFID implementations may not be worth those benefits.

In this paper, I evaluate the privacy implications of RFID applications in the hospital setting. Many hospital RFID applications have not been thoroughly discussed in the literature, and the proposed applications within hospitals are highly nuanced and varied. Some of them, for example, involve sensitive ethical issues relating to human tagging – meanwhile, others raise issues on how we should deal with extremely sensitive personal information. Indeed, RFID tags either store personal information or contain unique identifiers that can be linked to large amounts of data stored on servers. Any discussion of hospital RFID privacy requires an examination of various RFID hospital applications.

In addressing the privacy concerns that arise from the applications of RFID within hospitals, I employ a utilitarian framework that attempts to balance the usefulness of the technology with the privacy harms that are posed by it. The ultimate goal is not to justify deployments of RFID for RFID's sake – rather, it is to determine the privacy drawbacks to each RFID application while suggesting ways that RFID implementations may maximally alleviate privacy concerns. Such concerns may be alleviated via both legal and procedural means. In some cases, implementing RFID technology may be worth it if it provides benefits to individuals that outweigh a largely mitigated set of privacy concerns–in other cases, however, the privacy concerns may be impossible to overcome—or unknown—and those concerns may outweigh the benefits of the technology.

Once the decision is made to implement RFID in the hospital setting, there are several technological choices that will need to be considered. Some issues that have privacy implications include whether active or passive RFID tags are used, the type of information that is stored on the tags, the read/write capability of the tags, the encryption capability of the tags, and the frequency at which the tags operate. While these choices are beyond the scope of this analysis,

all of them have a direct bearing on the privacy implications of the technology, regardless of some of the legal and procedural recommendations considered here.

Because many hospital RFID applications are in pilot phases and have not yet been fully implemented on a large scale, it is impossible to legitimately analyze the full extent of benefits that each RFID application confers unto society. Further, the ultimate form of many RFID implementations remains unseen. While many hospital RFID applications have been proposed and implemented, future applications may alter the considerations that are made in this analysis. By addressing a wide variety of hospital RFID applications in this paper, I hope to address full range of privacy issues that may be presented by both present and future applications. These issues need to be brought out up front in order to ensure that RFID hospital implementations adequately tradeoff efficiency and privacy in both the near and far term.

This paper proceeds as follows. In Part I, I discuss the general arguments that justify RFID use in the hospital setting. Next, in Part II, I assess the literature on consumer RFID privacy, and use a proposed deontological framework to establish the principles that are used to evaluate various RFID applications. Further, I use the literature to confirm that the principles are consistent with those established by well-known privacy advocacy groups, and a discuss the principles in the context of the legal considerations that affect RFID policy. Part III provides the reader with some background on the few laws that currently govern hospital RFID in the United States, and, in Part IV, I then discuss several hospital RFID applications, providing recommendations on how we may best benefit from each application while ensuring the privacy of patients. Finally, I provide general conclusions and recommendations in Part V.

I. The Benefits and Costs of RFID in Hospitals

There are several reasons that RFID technologies are valuable within the hospital setting. Most importantly, the operational needs of hospital environment are well-suited to RFID. Standard hospital operating procedures, in particular, are improved by RFID because it can be integrated seamlessly into existing infrastructures. For example, medical instruments are subjected to extreme temperatures during sterilization. Although many technologies malfunction in the presence of such temperatures, RFID tags can tolerate them. Items within the hospital are also exposed to unique materials such as water, blood, and other materials. Since RFID signals can be designed to travel through such impediments, RFID can overcome those obstacles (Fishkin and Lundell 2006).

Given the fast-paced, cluttered environment that is the hospital, moreover, it is also essential that any new technology infrastructure does not present a significant burden to nursing staff, doctors, and other health care professionals. RFID facilitates this goal because it is non-obtrusive and easy to use. Its signals can travel through walls or floors, allowing readers to be stored in locations that are hidden from sight. RFID scanning, unlike barcode scanning, does not require direct lines of sight. This allows items to be identified with little or no action from hospital personnel. Further, RFID tags, even when expensive, are reusable for long periods of time (Banks et al., 2007, pp. 314-315).

Pilots within hospitals have verified that increases in efficiency are possible. This is unsurprising because the non-obtrusive nature of the technology prevents it from getting in the way of the day-to-day operations of the hospital. Data from RFID tagged patients shows that the technology improves medical processes, decision making, and resource management (Janz et al., 2005, pp. 132-148). A case study of a Taiwan hospital that used RFID to track SARS patients

found that an RFID has the potential to contribute to general operating efficiency, good medical service, and patient safety (Wang et al. 2006). A study from Cisco, finally, revealed that the implementation of wireless LANs within hospitals made hospital workers almost 27% more productive (2003).

A seamlessly integrated RFID solution within a hospital may also promote better patient care. If operating efficiency in the hospital is improved, doctors may have more time to interact with their patients, which would allow them to have more meaningful doctor-patient relationships. The University of Chicago Comer Children's hospital purchased an RFID implementation to "enable [its] staff to spend more quality time with [its] patients and less time manually performing administrative tasks such as billing and reordering" (Mobile Aspects, 2005, p. 1).

Much of the value from hospital RFID results from improved asset management. If assets are more effectively utilized in the hospital, costs are reduced significantly. Workflow management may also be improved. And, if an RFID system could quickly identify and locate pieces of medical equipment needed for a critical test or procedure, it prevents needless delays that may, in some cases, be the difference between life and death.

However, these benefits do not come without privacy costs. The tags may increase efficiency by not requiring a direct line of sight to be read, but this also means a malicious third party will have an easier time reading the information on a tag with his own reader. Sensitive patient information is either stored on the RFID tags themselves or on a third party database that is associated with the data on the tags. Should hospitals endorse a system that could expose the information on tags to such third parties? An additional problem is that, in some cases, hospital customers may not know that RFID technology is in their presence. Does a patient waive his/her

right to privacy when entering the hospital, or should zones of RFID use be clearly demarcated by the obvious presence of readers?

I ask whether these privacy drawbacks are worth the significant value proposition presented by proponents of hospital RFID. After establishing privacy principles, I provide the current legal landscape and discuss the tradeoffs associated with several proposed hospital RFID solutions.

II. Privacy Principles, Constraints, and Considerations

The focus of this work, ultimately, is on ways we may address the privacy concerns that are brought about by RFID opponents while still promoting the benefits that RFID could confer unto society. Because most implementers of RFID focus on generating new and interesting applications of the technology, they often fail to fully consider privacy principles that should guide RFID hospital implementations in the US. This section establishes these principles. In the next section, I apply these principles to the various applications that are discussed. I then consider them in the context of legal constraints that govern RFID in the US and support them by discussing the principles that have been established by the Electronic Privacy Information Center (EPIC)and the RFID privacy literature.

A. Establishing a Set of Overarching Legal Principles

To establish a set of principles that should guide our overall analysis, we employ a utilitarian framework that considers both the short and long term implications of implementing RFID technology. Since most patients would appreciate benefits that come from improved hospital efficiency and patient care, they would likely be willing to immerse themselves in an

RFID-enabled hospital. If patients demonstrate support of the technology, its use in the hospital arena should be allowed. This support, however, is subject to significant constraints.

First, endorsement of the technology in one area does not necessarily imply that it is endorsed by the public in all areas. Most Americans, for example, are not likely to be comfortable in a world that allowed them to be ubiquitously tracked on the streets or in their homes—and, as RFID applications continue to be pronounced, Katherine Albrecht and others argue that an imperceptible "RFID Revolution" could potentially permeate all of society (Albrecht and McIntyre, 2005, p. 219). Our principles, therefore, should not be susceptible to slippery slopes that facilitate additional RFID applications without the public's consent.

Second, acceptance of RFID technology in the hospital setting may not even represent true acceptance. Because of the uncertainty inherent in RFID's implementation, neither patients nor implementers of the technology can completely understand the overall implications of the technology's use at this time.

In particular, the major issue that we must consider in establishing our principles is the information asymmetry problem. A limitation of the utilitarian framework is that it assumes that individuals make fully informed, rational choices. However, when information asymmetries or uncertainties exist, these fully informed choices are not possible, and individuals are only able to go off of what they know and understand in making their decisions. In the behavioral economics literature, this is referred to as the availability bias. People generally construct their perceptions of likelihood based on the mental availability of instances of specific harms (Meyer, 2006, pp. 160-61). Absent explicit knowledge of privacy harms from RFID in the hospital setting, therefore, people will tend to underestimate its risks. Nevertheless, implementers of RFID will inevitably know a lot more about the privacy implications of the technology than will patients,

and they have an opportunity to communicate their understanding of the privacy risks to patients. Patients should thus have the ability to make choices relating to hospital RFID with the fullest information possible. As privacy scholars have noted, for example, "[n]ot knowing key pieces of information, such as which firms are interested in purchasing personal information and to what ends, disadvantages an individual so that rational evaluation of personal information-revealing strategies is impossible" (Magid et al., 2009, pp. 36-37).

The public knows little about RFID—it is a complex technology that is not widely talked about among laypersons. Poignant examples that indicate a lack of understanding appear in a study by Strickland and Hunt (2005). In this study, a general acceptance of RFID use for toll collection was revealed despite the fact that its associated data management practices were unknown. This is a problem, since states can easily use basic mathematical calculations based on RFID tracking to give speeding tickets and implicate criminals. If people know that their data could be used in this way, it is far less likely that they would accept the technology on face. Most merely see the advantages of speeding through the toll lane – and this is what they are told. We similarly fear that patients will only hear about the benefits of RFID in hospitals and accept it in a similar manner that does not allow them to maintain full information. And, unlike toll collection data, the information that could be collected using hospital RFID is far more sensitive.

This paper previously alluded to some instances in which RFID has already been piloted within hospitals. It is doubtful that there have been significant efforts within these hospitals to inform customers of the privacy risks associated with the technology. If patients continue to accept RFID hospital implementations without full information, we may be perpetuating a dangerous situation in which patients who obtain more information later on could retaliate. Indeed, patients may not have accepted RFID technology in a hospital setting had they fully

understood the privacy risks. As RFID continues to be implemented within hospitals, we fear that patients will eventually be forced to accept implementations of the technology *on-face* and without consent. Indeed, "[g]iven the growing prevalence of privacy-invading devices, individuals have succumbed to a sort of inevitability about disclosures" (Magid et al., 2009, p. 50).

This development is concerning because "inevitable disclosure" not only skirts around patient rights, but it also could lead to public frustration and retaliation that could have been prevented if the right steps had been taken in the first instance. Further, a sense of inevitable disclosure could cripple patients' sense of control over their personal privacy. To be legitimate, a fully-informed public should make a rational choice to be "on-board" the technology.

Implementers of RFID technology have the responsibility to make the technical design choices that are in the best interest of patients before implementing the technology. By making it a point to optimize patient privacy within the systems themselves, implementers will do their part to reduce impacts that could arise as a result of information asymmetries. Design choices in various facets of an RFID system should not be made blindly and without the consideration of privacy rights. In theory, systems that are perfectly designed would reduce the information asymmetry problem to a triviality since the system would then be "privacy perfect." However, such an assumption is overly optimistic – it is better to assume that our systems will not protect privacy perfectly and that we can complement privacy-friendly system designs with additional privacy safeguards. Moreover, regardless of the robustness of RFID privacy protections within a system, we must reinforce our notion of a fully-informed patient cohort that is required if we are to achieve a utilitarian ideal.

This means that regulation—and the law—has a role in ensuring that citizens are proactively educated about the privacy risks of various technological applications, including RFID in the hospital. This also means that consumers should be notified—both individually and collectively—when privacy breaches occur. Frequent notification may artificially inflate perceptions of privacy risks or trigger availability biases, but it would be normatively better for the public to overestimate privacy harms than to underestimate them.

There are several reasons a regime that overestimates privacy is desirable. Like Paul Schwartz (2009), I advocate a principle of first, do no harm. However, unlike him, I would not frame the primary harm as privacy regulation in the face of uncertainty which warrants a parsimony principle of minimal regulation (Schwartz, 2009, p. 928). Rather, the harm from the vantage point of one who wants the legal regime to accurately track society's privacy preferences would be a world in which the public's opportunity to express its privacy norms or values could be derailed by coerced acceptance or naïve reliance on privacy-harming technological advances. Daniel Solove (2009) explains that "the government could gradually condition people to accept wiretapping or other privacy incursions," which could artificially alter society's privacy expectations (Solove, 2009, p. 73). Further, governments—both federal and state—could under-regulate and fail to inform the public of privacy risks of emerging technologies. If this occurs, another form of coercion could occur as people gain reliance interests in technological innovations and become too invested in a particular application to recover the privacy rights they would have preferred to assert in the first instance. They also may succumb to the aforementioned sense of inevitability, and fail to push back on any harms arising from the technology for that reason.

Why overestimate privacy risks when doing so could undercut economic benefits or efficiency gains? The simple answer: the private sector will always be motivated to maximize profits. Absent regulation, however, they will not always be motivated to maximize privacy in a world filled with incomplete information. By erring towards a regime that overestimates privacy risks, we place a burden on industry to self-regulate the technologies and methods that are used to transfer and store information. If privacy harms are somewhat overestimated as a result of reduced information asymmetries between consumers and private actors, these actors will more proactively work to reduce the likelihood of privacy breaches in order to minimize the impact of perceived information privacy risks on their profits. Although consumers may still gain reliance interests in technological innovations and applications, increases in a technology's popularity over time will be a more accurate reflection of that technology's fully-assessed privacy risks. The market itself could solve for adequate privacy protection without the need for inefficient, *reactive* government regulation that would otherwise be necessary.

Assuming the provision of full information could ensure better measurement of society's privacy preferences, however, how should federal and state privacy law be balanced? First, hospital regulation at the federal level should always promote notification of information privacy risks and breaches in all sectors, especially for technologies or applications where privacy implications are uncertain. Privacy risk education could flow from a federal office or agency that studies the privacy risks and benefits of emerging technologies. It would be efficient for a single federal agency to perform such broad privacy risk and educational assessments instead of a patchwork of state notification and privacy research hubs.

The foregoing discussion reveals several principles that drive the remaining analysis of this paper. These principles should viewed with an eye towards conceptualizing privacy as a

form of personal property—as Schwartz argues, "[p]ersonal information is an important currency in the new millennium" (2004, p. 2056). It is therefore crucial that our privacy principles prioritize patient ownership over hospital (or private) ownership with respect to any RFID technologies that may incorporate the use of personal data—health or otherwise. The five property elements Schwartz describes—inalienabilities, defaults, right of exit, damages, and institutions—allow us to articulate these principles.

Principle 1 - Limits on transferability

Called *inalienabilities* by Schwartz, this privacy principle emphasizes that data obtained from RFID tags should be protected from arbitrary transfers to third parties. This principle emphasizes that the hospital patient always has ownership and dominion over the data. This means that implementers must first receive *opt-in* permission from someone who is tagged before their data can be used by that party. Moreover, this third party, upon being granted permission, cannot transfer or sell information about that person to others for any purpose unless authorized to do so. A single opt-in should not be viewed as an all or nothing proposition where a hospital or similar medical providers "assume[s] full control of information after consent is demonstrated . . . ." (Magid et al., 2009, p. 49). Treating information this way prevents individuals from making rational economic calculations about whether to reveal personal information. This principle arises out of a general concern that a market of transferable information is very likely to be made possible with the proliferation of RFID.

Principle 2 - Explicit opt-in defaults

There should be a default option that requires hospital patients to opt-in to any forms of RFID data use that may be associated with their personal information. Requiring patients to opt-in places the burden on implementers who will need to convince their customers to use the

technology. Presumably, it will lead to a more informed citizenry that is told why the technology is beneficial as well as why the technology has some potential drawback.

Three considerations should be emphasized when discussing opt-in defaults. First, opt-in defaults are only valid to the extent that they accurately reflect preferences and are not subject to the information asymmetry problem. Second, and as will be addressed in Part V, there are certain situations (infants, the elderly, and in the ER) where RFID hospital implementations may not be able to obtain legitimate "opt-in" from patients. Finally, to the extent that bifurcated systems can be maintained in the hospital setting—those that allow patients to use the RFID system while still allowing others to opt-out—such systems should be maintained.

Principle 3 - Right of Exit

Once someone opts-in to using the technology, there should also be a right of exit. Although someone may have felt that the technology was initially worthwhile, it should not be assumed that this initial consent gives the technology provider an unlimited right to use RFID to associate information with a person. Indeed, people may opt-in, discover things about RFID that they dislike, and then wish to opt-out of the technology. This is yet another reason why opt-in cannot be an all or nothing proposition. If customers do not have this right, we may reach a point at which a critical mass of consumers has little to no recourse against companies who fail to protect privacy.

Principle 4 – Right of Recourse

Invasions of privacy rights should be associated with some level of compensatory damages and ability to seek retribution for privacy harms that are inflicted on a particular person or group of persons. Although it may be difficult to pinpoint an individual who steals personal information or data using RFID technology in a particular case, a liability rule can be placed on

hospitals that fail to create the technological infrastructures that adequately protect privacy. Thus, even if a party outside of the hospital were to use technological know-how to steal patient data using an RFID reader, the affected person would always be able to secure recovery from a solvent party. Current privacy law sets liquidated damages that are quite steep to discourage violations – for example, the Video Privacy Protection Act allows a court to "award … actual damages but not less than liquidated damages in an amount of $2,500." People should know about their right to seek recourse—whether it be from the hospital itself or from the individuals who steal personal data.

Principle 5 – Institutions that Ensure Full Information Provision

Institutions should be created that regulate and enforce RFID privacy provisions. Schwartz advocates the creation of a Data Protection Commission that would fill a more general oversight function. The United States is the only large Western nation that has failed to create such an independent privacy commission (Flaherty, 1989, pp. 394-97). Consistent with the discussion above, one major role of such a commission would be to ensure that consumers were armed with full information. Thus, it would ensure that consumers had notice of the presence of RFID technologies in hospitals, that accurate information about the technology was communicated, and that consumers have an authentic choice to opt in and out of the technology as they please.

B. Supporting the Principles

Assuming the above principles are adopted, they must withstand the scrutiny of both the general public and consumer interest groups. This section compares and contrasts these principles with those that have been articulated by various privacy groups.

First, we examine the privacy principles established by EPIC regarding health information privacy. Marc Rotenberg, EPIC's President, gave a talk in 1994 entitled *Privacy and Security for Medical Information Systems*. In this talk, he emphasized several principles that can be applied to RFID in the health care industry. These principles emphasized a code of fair information practices, controlling secondary use, controlling the use of an identifier, patients' right of access, and oversight and enforcement.

Each of EPIC's principles can be associated with the general principles introduced above. First, a code of fair information practices emphasizes the responsibility of data holders to their subjects, and, in addition, the duty to keep data subjects fully informed about the use of their personal information. This principle is somewhat connected to the principle of opt-in defaults because these defaults have the primary goal of forcing data holders to share information with their subjects, but neither such codes nor such defaults are enough. These measures do not ensure that consumers are fully informed about privacy and the use of their data. As such, it is important that any opt-in policy is coupled with other safeguards to ensure that fair information practices exist and are met.

Second, EPIC recommended in 2005 to the Department of Health and Human Services that RFID implementations in the healthcare setting should contain the minimum data possible to function effectively. This is a technical consideration, as the amount of data stored on tags and servers is a system design choice. Minimization measures would promote the principle of inalienability.

Another important consideration noted by Rotenberg, finally, is controlling the use of identifiers. All RFID tags have identifiers that—using either a random number or some other combination of data—serve to identify individuals or items that are associated with the tag.

Although the context in 1994 was different—the goal was solely to address identifiers within medical record databases—the controlled use of identifiers is *even more critical* in the RFID world because so many RFID implementations in hospitals emphasize the use of a unique ID to be associated with tags on each item or patient. Such a unique ID needs to be chosen carefully and implemented in a proper way. For example, were a social security number chosen as a unique ID in an RFID implementation, a malicious third party could intercept that information and use it to exploit that person's banking and credit records. This too promotes the inalienability of patients' private data.

Beyond EPIC, Lisa Sotto, former vice chair of the Data Privacy and Integrity Advisory Committee of the US Department of Homeland Security, advocates the adoption of an RFID Code of Conduct in the medical industry. Although HIPAA, federal and state laws, and the Fair Information Practices established by the FTC provide some privacy protections that cover RFID implementation in the healthcare field, she believes that such a code of conduct would offer an additional layer of protection that would be more specifically and clearly tailored to address specific concerns about RFID (Sotto 2005). Indeed, such a code of conduct has recently been created by the American Medical Association in the context of implantable RFID chips created for medical use (Bacheldor 2007). Such a code, however, doesn't extend more broadly to other hospital RFID applications.

Upon a simple examination of each portion of Sotto's proposed code of conduct, it too is almost directly in line with our established principles. It would require notice, opt-in, and the ability to review and amend data stored on the tag. Further, Sotto's proposed code would call for instruction on chip deactivation, which would be another way that patients could exercise a right of exit. Finally, she also emphasizes accountability and enforcement. These ideas are all

consistent with the notion that RFID data is the personal property of hospital patients and not the hospital.

III. Legal Considerations

Currently, there is little law that affords consumers privacy protections with respect to RFID implementations in hospitals. Although the Fourth Amendment of the Federal Constitution prohibits "unreasonable searches and seizures," the Supreme Court has long established that the Fourth Amendment only applies to government actors (Sommer, 2009). Thus, the Constitution places no limits on private hospitals or medical providers. Further, there are not any Federal statutes that directly address RFID privacy issues. As Paula Bruening of the Center for Democracy and Technology has noted:

> It is more effective and efficient to begin at the outset of the development process to create a culture of privacy and that establishes the key business and public policy decisions for respecting privacy in RFID use before RFID is deployed rather than building in privacy after a scandal or controversy erupts publically (Bruening 2004).

Nevertheless, some federal legislation addresses RFID hospital privacy indirectly. In addition, bills addressing RFID-related issues have been proposed at the state level.

A. Federal Legislation and Regulations

The main bill that is referenced when discussing RFID privacy concerns is the Health Insurance Portability and Accountability Act of 1996 (HIPAA). After HIPAA was passed, it was amended to include *Standards for Privacy of Individually Identifiable Health Information*, also known as the "privacy rule." The privacy rule sets forth several guidelines that control how

medical patients' personally identifiable information may be distributed. This personally identifiable information is known as "protected health information (PHI)."

The limitations the rule presents on PHI have several implications on RFID implementations. And because HIPAA applies to "any health care provider who transmits health information in electronic form…," it applies to hospitals.

The privacy rule implicitly requires that PHI be stored in centralized databases and not on RFID tags themselves. This is because the privacy rule protects PHI held in any form of media, and the information stored on RFID tags is susceptible to third party adversaries who may attempt to read it. Even in the presence of encryption, a third party with the proper decryption tools could, in theory, collect patient information with a specially designed reader. By storing the PHI in central databases within a given health care facility, the information is not accessible within public areas, and this provides an extra layer of protection of third party intrusion. The ubiquity of RFID in the hospital setting facilitates many points of entry for the random hacker who could attempt to collect information from individuals who may be tagged (whether the tagging is under the skin or via a bracelet).

The information protected under HIPAA extends beyond medical information about a given patient. This is because the protected information can also include information that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual (45 C.F.R. § 160.103 (2009)). Thus, even if an RFID tag does not contain any medical information about a patient, the identifier on an RFID tag must also be protected. Thus, identifiers on tags such as social security numbers, phone numbers, or publicly available hospital identification numbers may not be used to identify a patient who may be tagged with RFID. Only "de-identified" information may be included on tags, and the propriety of using such information

must usually be verified via a formal determination by a qualified statistician (45 C.F.R. § 164.514(b) (2009)). As studies have shown, however, de-identification is virtually impossible since seemingly de-identified data may be re-identified in some instances (Sweeney, 1998).

Although the use of the protected health information is regulated, this regulation does not extend to all uses of PHI. In general, the PHI cannot be disclosed unless the individual who is the subject of the information (or the individual's personal representative) authorizes such disclosure in writing. The information can also be disclosed by the entity that holds the information for the purposes of its *internal* treatment, payment, and health care operations (no disclosure to third parties). However, hospitals must also disclose the "protected" information to the US Department of Health and Human services when it is undertaking a compliance investigation, as well as to certain entities for "national priority purposes"—these may include law enforcement and public health activities (45 C.F.R. § 164.502(a) (2009); 45 C.F.R. § 164.512 (2009)).

Finally, the privacy rule requires that medical providers provide a notice of their privacy practices. Given our consistent stance in this paper regarding the right of individuals to be fully informed, we believe this is a good requirement. There are specific provisions that, for example, require the privacy notice to be descriptive in the ways the provider may use and disclose personal information. It must inform patients of their rights, including the right to complain to HHS (45 C.F.R. § 164.502(a)-(b) (2009)).

Moreover, one additional federal law may be construed to apply to RFID technologies in some circumstances (Sommer, 2009). The Electronic Communications Privacy Act (ECPA) regulates electronic communications. ECPA makes it a crime for any person who, "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication" (18 U.S.C. § 2701 et seq. (2009)). To the

extent that intercepted communications between an RFID tag and reader are construed as "electronic communications" under the act, one could argue that ECPA applies. Courts have not resolved this matter, however.

Finally, federal regulatory agencies—including the Federal Communications Commission (FCC) and Federal Trade Commission (FTC) have addressed some RFID issues. The FCC, for example, can regulate RFID through its regulatory authority over the frequency spectrum. Thus, it may allocate particular frequency ranges to RFID uses. For example, operation in the 433.5-434.5 MHz band is restricted to RFID uses "limited to commercial and industrial areas such as ports, rail terminals, and warehouses" (47 C.F.R. § 15.240 (2009)). Further regulations can explicitly expand particular portions of the spectrum to hospital RFID applications.

The FTC, meanwhile, issued a report in 2005 discussing the implications of RFID applications on consumers. Although the FTC does not currently have the authority to issue formal RFID privacy regulations, it argued that "the goal of such programs should be transparency," and that notice should be "clear, conspicuous, and transparent" (FTC, 2005, p. 22). It concluded that "consumer education is a vital part of protecting consumer privacy" (p. 23). Although the report highlighted the fact that industry regulations can play a role in this area, the FTC would serve the public well by educating the public on these matters.

B. State-Level Laws

Although several state laws have either been proposed or are on the books, most of these do not address RFID hospital privacy matters in a comprehensive fashion. According to the National Conference of State Legislatures (NCSL), thirteen states have passed RFID legislation as of 2010.

Of these current laws, four of them directly address RFID chip implantation. As I discuss later, chip implantation may be an effective tool to improve medical efficiency. Nevertheless, some are quite fearful of the ethical and moral implications of chip implantation. Thus, employers or other institutions are not allowed to require chip implantation of their employees or patients (National Conference of State Legislatures, 2010).

Most of the other laws, however, are less directly connected to RFID hospital privacy issues. Many are concerned with RFID use in drivers licenses or passports. Nevertheless, some of these laws bear some relevance. For example, Michigan's RFID privacy law governing RFID drivers licenses adopts the principle of minimization by only allowing a since unique ID to be stored on the license—it is also encrypted. Moreover, there is a notice provision. An applicant must sign a declaration acknowledging an understanding of RFID technology before an "enhanced" drivers license is issued (Mich. Comp. Laws § 28.304 (2009)). Nevada, in addition, has a law prohibiting the malicious capturing, reading, or storing of RFID information on a form of identification without the person's knowledge or consent (Nev. Rev. Stat § 205.461-205.4675 (2009). To the extent that these ideas can be transferred to legal requirements governing hospital RFID, state legislatures have had some good ideas.

Although RFID related legislation has not been proposed without controversy or mild shortcoming, this legislation is promoting a public discourse that will allow privacy and other concerns to be vetted out.. In New Hampshire, such dialogue has already occurred, as the originally passed bill was sent back to the house from the Senate, and was amended to create a privacy commission that will investigate RFID privacy issues further. This privacy commission released a report in 2008 that contained many useful recommendations. Although they did not discuss hospital RFID, the report proposed regulations that directly addressed chip implantation

and illegal uses of RFID readers (2008). These sorts of conversations and reports could help move additional reform forward.

C. Opposition to Legal Remedies

Despite the seeming power of legal measures to enforce RFID privacy, sheer passage of laws will not necessarily guarantee the privacy of hospital patients in the United States. If the public and consumer privacy advocates do not support such laws, they may not be taken seriously. And, if doctors and medical practitioners do not support laws that protect RFID rights, it is unlikely that the laws will be enforced. The FTC report on RFID technologies, further, emphasized the importance of industry regulation (2005).

Any incremental legal protections that are analogous to the HIPPA rule will need to be justified to physicians to be effective. In a 2005 *Health Affairs* article, Slutsman et al. released the findings of a study that revealed significant discontent among doctors when it came to the privacy rule. Despite being very familiar with the privacy rule, for example, only one of four physicians felt that medical record privacy is a serious problem. Meanwhile, a minority of them believed that the privacy rule helped maintain the privacy of medical records. Some (roughly one-third) believed that the rule would *impede medical research* (Slutsman et al., 2005). This has negative implications because, besides indicating that the rule may be ineffective, studies have suggested that physicians will ignore or not fully implement legal requirements that they do not agree with (Siegal et al., 2001, pp. 63-78). Such ignorance could produce frustrations that hinder quality of medical care.

Nevertheless, the study did also find that organizations with more procedural privacy practices in place were about seven times more likely than those with fewer provisions to do a very good job at protecting privacy, and also that such organizations were about five times more

likely to *not interfere* with physicians' abilities to care for patients and consult their colleagues (Slutsman et al., 2005). Thus, while there may be a general frustration with additional legal privacy protections on the part of doctors, effective compliance with the provisions probably is in the best interest of patients. Nevertheless, the effectiveness of the law should be continually examined, and something should be done to counteract the negativity doctors have expressed towards efforts such as the privacy rule.

Because of the general discontent doctors have expressed towards legal privacy protections, it will be especially important to educate doctors and other medical personnel—not just patients—on RFID technology before undertaking any RFID deployment. The median age of doctors today is quite high, and it is likely that most of these doctors will not understand or have much of an interest in this technology. Thus, any additional red tape related to the technology (i.e., red tape that protects *even more* privacy that may be needed due to an RFID implementation) is likely to frustrate or confuse many American doctors. While this red tape may be burdensome to physicians, they are more likely to be accepting of it when they fully understand the rationale behind it.

Beyond doctors' discontent, Katherine Albrecht and Liz McIntyre (2005) argued in *Spychips* that government and legal intervention in the RFID privacy realm is not a viable solution. They contend that there is a lack of political willpower to go against RFID, citing a Republican Taskforce that stated that "RFID holds tremendous promise…and should not be saddled prematurely with regulation." Meanwhile, Congressmen have funneled American tax dollars to support RFID research (pp. 204-205). From examples such as these, Albrecht and McIntyre assume that lawmakers will succumb to corporate pressures, refusing to support any legislation that limits RFID usage. To date, their prediction has been realized. As this section has

illustrated, federal RFID privacy legislation is minimal at both the federal and state level. Nevertheless, much of the problem remains a general lack of awareness of the technology's wide-ranging implications.

At this time, most patients who have received implantable RFID chips are sufferers of Alzheimer's disease, diabetes, and other chronic illnesses (Banks et al., 2007, p. 316). But use of such chips could proliferate. For this reason, government intervention should complement any efforts the public may take to assert RFID privacy rights. In particular, the government should maintain a role in information provision. It is unrealistic to assume that a substantial proportion of the public will appreciate the nuances of their privacy rights, just as it is unrealistic to assume that a substantial proportion of the public will be able to name their Congressional representative. And, while most consumers of RFID would probably be concerned if they truly understood the privacy issues that are intertwined with RFID, most are completely oblivious to the concept.

Despite the substantial privacy concerns associated with the implantable VeriChip, for example, the public has only become more supportive of the chip. Although only 9% said they would put it in their bodies after the initial announcement, 19% said they would after FDA approval. And, once Tommy Thompson joined the VeriChip board, the rate went up to 33% (DeNoon 2005). Corporations who are creating value-added solutions with high profit-margins are not necessarily going to listen to the relatively small number of consumers who actively voice their concerns against RFID. Absent a catastrophic event involving an individual's—or group of individuals'—compromised privacy, consumers are unlikely to exercise broad, concerted action independently.

Although Gillette, Proctor and Gamble, and others have succumbed to consumer pressure to back away from consumer deployments of RFID, such scenarios are less realistic in the hospital setting. Medical care is unlikely to be resisted by consumers in moments of urgent medical need. While people can easily switch between products in the supermarket that may or may not be privacy friendly, it is not so simple to switch hospitals or medical providers on a whim.

Most importantly, the reality is that RFID is being implemented in hospitals *right now*, and whether or not that reality is desired by privacy advocates, it needs to be acknowledged. The time frame to coalesce enough citizens to have an effect on corporations is far too great, and the only way corporations will begin conforming to privacy guidelines will be by strengthening our laws.

IV. Introduction of Hospital RFID Applications

We now turn to a discussion of many of the proposed RFID hospital applications. With the exception of the first application we discuss (asset management), most of these applications have not been formally implemented within any major hospital. We therefore hope to create an awareness of the potential uses of RFID based on what we know right now – however, the uncertainties associated with the technology may mean that the technology is *never implemented* in some of the ways described. Meanwhile, there may be future hospital RFID applications we do not consider here. These examples mainly serve to contextualize many of the privacy issues that arise from implementing RFID in the hospital in different ways.

A. Asset Management

The first major use of RFID in the hospital setting is for asset management. Hospitals are often lent assets such as hospital beds or monitoring equipment that are owned by third-party vendors. Such third party vendors would like to have the ability to track their property. In addition, some hospitals own their own machines, beds, surgical tools, and other equipment, and the internal tracking of such items can be quite useful in any efforts to bolster the overall efficiency of hospital operations.

Asset management has been the most pioneered application of RFID in hospitals because the primary incentive motivating RFID implementations is a positive return on investment (ROI). In an interview with Dr. In Ki Mun, a hospital researcher at MIT, we were told that the primary implementations of RFID at the hospital level are in asset management because the ROI for this application is estimated to be particularly high – in a mere 2-3 years, investors can expect positive returns. Meanwhile, Mike Dempsey, the founder and CTO of Radianse, claims that a deployment using their systems typically has a breakeven ROI somewhere between 11 and 18 months (Goth, 2006). These time frames are short enough to appease members of hospital boards to invest now.

A survey of the literature on RFID in hospitals verifies this. As early as 2004, Agility Healthcare Solutions made a five year pact with three Virginia hospitals to track mobile hospital equipment. In one of these hospitals (Bon Secours), it was estimated that a positive return on investment would be obtained within one year of deploying the system. This is unsurprising because, according to the CEO of Agility Healthcare, equipment management is a "universal problem in hospitals" (Collins 2004). One of the highlighted advantages to the Agility implementation is that its readers are linked wirelessly to the hospitals central networks, allowing reader positions to be reconfigured without reinstalling cabling. This is beneficial since hospitals

reconfigure layouts frequently. Several other hospitals, including Beth Israel in Boston, Washington Hospital Center in Washington DC, continue to use RFID to track assets (Brown, 2007, pp. 157-58).

Many in the hospital field doubt the economic viability of hospital RFID implementations, even in areas of asset management. According to Provizio Research in 2004, most hospitals expressed a desire to rely on bar code technology for at least six years. The main reason for this was that it was difficult to justify the cost outlay for "the more expensive, but clearly promising, RFID technology" (Jaques, 2004). And although RFID can be more easily integrated into existing infrastructures than before, the current IT infrastructure of most hospitals still makes it easier to use bar codes.

In September 2005, moreover, a similar study by Spyglass Consulting group revealed that RFID – particularly passive RFID – is not ready for use in the healthcare sector. In interviewing more than 100 healthcare organization professionals, that study revealed that less than 23 percent of RFID healthcare solutions are passive,[1] and that many of these professionals did not see a strong business case for the passive RFID due to the cheaper bar code alternative, a lack of industry standards, and a lack of government or industry mandates. Many also expressed concerns about expanding existing network infrastructures and about the scalability of the technology – there is a desire to use existing wireless networks over using an independent, dedicated RFID network (Monegain, 2005). But these concerns have been addressed in current implementations—both Alexandra Hospital in Singapore and Jacobi Hospital in New York utilize viable active tag implementations, and Beth Israel has successfully deployed its system over its standard 802.11 wireless network (Brown, 2007, pp. 157-58).

[1] Passive RFID tags do not have their own internal power sources. They are powered by the signals that are read by the tags and have short read ranges. Active RFID tags, on the other hand, are powered by their own battery sources and can propagate signals much farther than passive RFID tags.

Ultimately, there is general agreement that RFID will eventually replace barcodes. This is because the potential advantages to it are so substantial. Besides the utility asset tracking gives a hospital in terms of item recovery and efficient operation, asset tracking may also allow for applications that may benefit the hospital in other ways. For example, some hospitals have attempted pilots where they tag medical practitioners and associate these practitioners with objects for educational purposes. In a pilot with the University of Washington Medical School, students wore small RFID readers in a glove – two antennae in the gloves allowed for easy tracking of the sequences of objects used by students in simulations. The records of such sequences can be used to assess student performance, and this is one of many ways that RFID may be used to not only monitor behavior in the hospital, but assist it as well. If, for example, a student picked up the wrong tool for a given operation, an alarm could sound that guarantees that another, more experienced doctor may properly intervene. In this sense, RFID adds another layer of protection against medical error (Fishkin and Lundell 2006).

The application of RFID in hospital asset management is relevant to our privacy discussion for multiple reasons. First, the continued use of RFID for asset management will certainly pave the way for the use of RFID technologies in other ways that may more directly impact patient privacy. By creating RFID-enabled infrastructures within hospitals, for example, asset management applications will make it easier to move towards a system that integrates human tagging. Second, there are some direct patient privacy implications to consider at the asset level. While the tracking of general assets such as monitoring devices and hospital beds may not appear to impact patient privacy, there are ways that directly tracking patients will have such an effect. For example, a tracked hospital bed may be associated with a patient who sleeps in a bed during a given night. Meanwhile, the device that monitors that patient's heart rate can also be

associated with the patient as it is wheeled around the hospital with the patient attached. As such, measures must be taken by hospitals to ensure that such associations are not made without the knowledge or consent of a patient. In these instances, patients should know that RFID is being used and tracked items should not be directly associated with patients without full information and consent.

Despite the potential infringements of patient privacy that may result from asset management applications, they are minimized if these assets are never associated with particular patients. However, such a sweeping policy is only possible when discussing asset management for *general hospital assets.* The unique nature of the hospital environment also promotes another form of asset, which we call *patient assets*. *Patient assets* are different from general assets because they must be associated with patients to be used effectively in the hospital. Because such associations are inherently necessary with patient assets, we must address the additional privacy concerns that arise.

Two hospital RFID applications involving *patient assets* - hospital blood inventory and patient pharmaceuticals – have both been considered and implemented in pilot forms. We therefore address these applications in the following sections. A third patient asset, breast milk, is addressed in a later section on neo-natal intensive care units.

B. Hospital Blood Inventory

Current processes for hospital blood transfusions involve both paperwork and the use of bar codes. These processes have generally worked to this point, but proponents of using RFID in hospital blood inventory procedures argue that RFID could greatly improve the efficiency of such processes. The line of sight requirement of bar codes, for example, slows down hospital blood inventory processes because it requires that, in some cases, many bags be individually

scanned to find a correct match to a particular patient. RFID tagging would allow many blood bags to be queried at once, making it easier to track down and locate a blood bag that may be needed for a transfusion. Moreover, RFID tags are less susceptible to wear than are bar codes, and their use can increase general staff mobility and efficiency, improve data collection, and increase general hospital staff access to blood data.

Because blood-handling processes currently require a number of manual steps which may be eliminated with RFID, proponents also argue that RFID would reduce errors that result from the blood transfusion process. Errors in the blood identification process, meanwhile, can have very harmful effects. This is because incorrect blood transfusions sometimes lead to death or the transmission of harmful diseases such as hepatitis or HIV. While erroneous blood transfusions are known to occur at a rate of about one in every 12,000 units, experts argue that the error rate is actually much higher since many “near miss” incidents go unreported. In a 6-month RFID blood tagging pilot at San Raffaele Hospital in Italy, *no errors* were observed in the blood transfusion processes that were part of the pilot (Dalton et al., 2005).

In the pilot at San Raffaele hospital, the following procedures were used during blood donations and transfusions. For a transfusion, patient information, including a photograph, was stored on wristbands that were given to each patient that entered a blood donation area. The relevant data on these tags would then be copied to the blood bag tag that corresponded to the donation. After the donation is made, finally, the staff member compares the full blood bag and wristband via a personal digital assistant. Assuming patient data is initially written to the RFID tag correctly, this procedure ensures that the correct blood bags are associated with the correct patients. For a transfusion, patient data on a wristband is matched with the data on the blood bag

for verification, and the transfusion takes place. If the match fails, an alarm sounds and the transfusion does not take place (Dalton et al., 2005).

Because blood transfusion involves patient assets, we must be much more rigid in our privacy analysis of this application. In the San Raffaele pilot, there was no discussion of an opt-in default whatsoever. Any patient who was either donating or retrieving blood from the blood bank there was automatically subjected to the use of RFID-tagged blood. Implicitly, there was no right of exit in this implementation either, since all patients who used the hospital for blood transfusion needed to go through the RFID pilot. However, especially in the context of pilots such as these, it is not difficult to give patients the option to store their blood either with or without RFID tags – blood bags had been identified without RFID for years, and hospital personnel understand the procedures involved. Patients, meanwhile, should at minimum know that the blood they are donating is tagged – it didn't appear that those involved in this pilot were told about what was going on behind the scenes. These steps need to be taken sooner rather than later to ensure that a fully informed citizenry accepts the technology.

Meanwhile, because we know the specifics of this RFID system, certain aspects of it concern us because the design does not take care to minimize privacy risks. In particular, the tags that are associated with patients did not contain the minimum information possible. The tags in the system contained information about the patient's blood type, a picture, and other personally identifiable information. While this may have made it easier for system designers – for example, this design could make it easier to cross-checking blood samples with patient records – this particular aspect of the design is worrisome. The tags associated with blood bags could be designed to protect privacy much more if they only contained unique identifiers associated with given samples of blood.

Moreover, the tags that were used in this implementation were writable – information about a patient and their blood type was written to the tags during the process of tagging and identifying blood samples. By using tags of this nature, there is room for third party adversaries to write invalid or mischievous information to tags. While this would appear to be an unlikely possibility, it is something that could legitimately happen and this is a flaw in this RFID implementation.

C. Patient Pharmaceuticals

Another application on the horizon involves the tagging of patient pharmaceuticals. In hospitals where thousands of medications are administered on a daily basis, it is important that the correct patients receive the correct medications. Because RFID aids in verification procedures, it could serve as an extra layer of protection in ensuring that incorrect drugs are not administered to patients. Moreover, it is also important that patients receive the proper dosages of their medications, and RFID systems can help gauge how much medication patients are taking. In a society that is increasingly concerned about the presence of counterfeit drugs, positive identification of all drugs is a pressing issue.

CVS Pharmacy has been a leader in the tagging of pharmaceutical products through its participation in an RFID trial called project Jump Start. CVS was interested in the project because over 70% of its revenue stems from prescription drug sales. In addition, CVS wanted to get on board early to ensure that any RFID standards made with respect to pharmaceuticals considered the *specific needs* of pharmacy retailing – these needs include a consideration of the specific privacy and security requirements of pharmacy retailing (Garfinkel et al., 2005).

Project Jump Start uses electronic product codes (EPCs) to track shipments of drugs, and it is possible that these individual EPC codes could be associated individual customers.

However, the initial roll-out of Project Jump Start has only tagged bottles that contain 90-100 or more tablets – these are the bottles of pills that are broken and placed into smaller bottles by pharmacists. The tags used in this project, moreover, have an adhesive backing and perforations that make them easily removable by either the pharmacist or consumers. By taking these steps, CVS has implemented its pilot in a way that can still increase efficiency in the supply chain while avoiding infringements of privacy at the consumer level. However, one can't assume that all implementers of pharmacy RFID will act like this. CVS was cognizant of privacy, going so far to say "if people [developing this technology] don't understand privacy, this thing is going to be stopped dead in its tracks" (Garfinkel et al., 2005).

In general, there are several privacy considerations in using RFID with pharmaceuticals. First, a system that contains RFID tagged prescriptions must not allow adversaries to associate customers' prescriptions with specific customers – this is because pharmaceuticals, like blood bags, are patient assets. The ability to know who is prescribed what medicine has immense privacy implications because, beyond knowing the medication itself, the adversary would also be able to infer diseases or medical conditions that are afflicting a customer or members of a customer's family. Moreover, all forms of *personally identifiable* medical information are protected under HIPAA. Thus, CVS could face legal trouble if it installed a faulty RFID system.. Finally, consumers should have the right to *opt-out* of an RFID tagged prescription upon purchase.

Although CVS could improve privacy by taking some of the steps above, it only deals with consumers who purchase drugs at its stores, and its primary goal is to improve supply chain efficiency. While the same motivations may exist for some who are in charge of hospital pharmacies, hospitals may have a broader interest in tagging pharmaceuticals. Tagged

prescriptions, for example, could be associated and verified with patients at bedside by nurses who may be administering drugs. This, in fact, could eventually become standard practice within hospitals as it becomes the most efficient and cost-effective thing to do. Because of this possibility, patients should understand that these future implications of tagging pharmaceuticals, and they should be given an option to not use them. Because drug information is already printed on bottles, and patients frequently administer drugs to themselves, there is not a strong argument for tracking prescription bottles throughout the hospital. Even if there is some marginal health "gain" to be realized by individual patients by tracking their drugs, an educated patient should be able to make an informed decision as to whether or not he wants his drug bottle to be tagged.

Despite these concerns about broader tracking of prescriptions within the hospital, there may be legitimate reasons for tagging pharmaceuticals. For example, if drugs are to be taken by patients at certain times of the day, or there is a limit on how many times a drug should be administered to a patient, RFID may be a valuable tool to identify that a prescription bottle was taken from the patient's bedside at the wrong time of the day. This could sound an alarm that informs nurses that a patient may have improperly taken a drug. It also may be useful for patients who take several prescriptions and must keep track of all of them. However, we believe that measures beyond RFID can be taken to solve those types of problems. This is because most patients are capable of reading labels and administering drugs to themselves, and the efficiency gains from this use of RFID tagged pharmaceuticals do not appear to be great. The tracking of such drugs within the hospital may be a more feasible option for those who are incapacitated or face unique challenges, but this still doesn't provide a reason to track pharmaceuticals absent consent and adequate privacy protections.

Overall, while a well-implemented RFID blood inventory system could improve hospital efficiency and provide a good service to patients and the hospital, the tagging of pharmaceuticals should be primarily used for inventory management in the ways employed by companies such as CVS. Once a hospital pharmacy is assured that it has the correct drugs, it does not make sense to make associations between pharmaceuticals and patients within the hospital who are prescribed to receive those drugs, especially given the privacy risks that could result from tagging patient assets.

D. Tagging of Humans

There are several types of "human tagging" that can be implemented within hospitals. First, the tagging can occur at two distinct levels, since tags can either be external in the form of a wearable device or internal implants under the skin of the patient. This external tagging is occurring in hospitals right now: Alexandra Hospital in Singapore that tracks all "patients, visitors, and staff entering the hospital" using an ID card (Brown, 2006, p. 157). Jacobi Hospital in New York, moreover, issues wristbands encoded with a patient ID number to all patients upon check-in. These wristbands are accessed by tablet computers that have their own RFID readers.

The circumstance of a patient who is tagged is relevant in discussing privacy. For example, the circumstances surrounding a patient who is casually admitted to the hospital are distinct from those surrounding someone who is urgently rushed to the emergency room. Circumstances surrounding the tagging of children and the elderly differ as well. We therefore examine several different forms of human tagging in our analysis. We first discuss the privacy measures we believe should be considered for implantable versus external tags, and then go into the issues of tagging different people facing different circumstances.

1. Implantable RFID – the VeriChip

While the tagging of babies, the elderly, and other humans has presented some concerns, the most controversial of all applications has been *implantable* RFID. This is the one form of RFID in the medical field that has been explicitly banned by state statutes. The *Verichip* is an implantable device that is about the size of a grain of rice that contains a unique ID number. Proponents argue that this device has invaluable applications to the medical field because it can be used as a fail-safe identifier in the case of an emergency. If, for example, a person is unconscious upon arrival to the hospital emergency room, that person can still be easily identified in the event that the hospital has a *VeriChip* compatible reader. The chip's unique identifier can be associated with a database that contains a person's medical records, ensuring that the hospital properly obtains a person's blood type, medication history, and other important information. And, according to Arthur Caplan, director of the Bioethics center at the University of Pennsylvania, "you are more likely to die or be harmed by lack of medical information about you than by people knowing too much about your medical information – in an emergency, it's important for doctors to know what your allergies and medical problems are…." (DeNoon, "Chip Implants", 2005).

Moreover, this chip may be used to identify elderly patients - those suffering from dementia or Alzheimers disease. An example of this is described in a March 2006 Washington Post article, in which Roxanne Fischer explained that she had the *VeriChip* implanted in her 83 year old mother. Roxanne did this in case she could not be reached in the event of an emergency, and implanting the device in her mother gave her "tremendous peace of mind." Although few people have implanted the chips as of now, *VeriChip* has offered extensive incentives to hospitals to deploy the infrastructure for the technology – for example, it provides free readers to

hospitals that sell the chip (Stein 2006). A new company, PositiveID, now holds the rights to the *VeriChip*.

Overall, this particular application has not been received well, and the reasons for this are clear. First, such chips could make it easier for unauthorized third parties to access medical records. Mainly, however, some fear that the chips will lead to an Orwellian society in which individuals are constantly monitored – unlike other solutions, the chips are permanently readable and cannot be turned "off." Moreover, people like Richard Smith (Internet and privacy consultant in Boston) say that "it's not a secure chip – there's nothing to stop someone from accessing the code and cloning the chip to access records." In fact, Westhues cracked the *VeriChip* in less than two hours in 2006 (Ulatowski, 2008, p. 647). Finally, who can access the databases that store medical information? Given a unique ID and access to PositiveID's VeriMed database, it is not difficult for a third party to obtain someone's medical records. This, actually, is a problem with all centralized databases. While PositiveID claims that privacy is its utmost priority, its interest is undoubtedly also to make profit. We therefore must assess some of these high level concerns with respect to the *VeriChip* sooner rather than later. This is especially true as the technology becomes increasingly popular – at a medical convention in 2006, 172 new physicians elected to offer the VeriMed ID system (and therefore the *VeriChip*) to patients, representing a 300% increase over its previous adoption (*VeriChip* Press Release, 2006).

Despite concerns with the VeriMed system, however, *VeriChip* and its successor corporation have been mindful of privacy. The *VeriChip* tag only contains a random identifier that does not contain any personal information, and one must explicitly opt-in to receive the chip. Although the chip is implanted, there is an opt-out possibility since the chip may be removed through a "simple procedure." Depending on a patient's privacy preferences, moreover, the

patient may choose the extent of data stored on the VeriMed servers. Finally, because the VeriMed system employs passive tags, tracking is difficult because a reader must be within 2.5 inches of a person to read the tag.

Under our utilitarian framework, however, we desire that full information is provided to patients regarding the *VeriChip*'s overall implications. For those RFID applications that will stay within the hospital's confines (wristbands, tagged blood etc.), these implications do not usually extend beyond the hospital, and the information provided may not need to be very extensive. However, the privacy implications of *VeriChip* extend beyond the hospital domain and to areas well outside the hospital – this is especially due to the difficulty of "turning off" the chip absent a medical procedure.

With *institutions* that enforce standards of system design to ensure privacy, we hope that approval of RFID hospital systems will eventually be more stringent and that we may prevent many privacy issues before they happen. It is dubious that the FDA, in approving *VeriChip*, undertook a broad consideration of its privacy implications during the approval process. And, because *VeriChip* has not seen widespread implementation yet, we are uncertain as to how broad the privacy effects from its current design will be. Because of these uncertainties, and the *potential* for particularly strong privacy effects in this case, we need strong institutions along with laws that maintain patients' rights to seek compensatory damages if they are misinformed.

2. Neo-Natal Intensive Care Units

One of the more tailored RFID applications that has been considered within hospitals is that within neo-natal intensive care units (NICUs). This is because NICUs present several unique challenges to patient identification. Unlike a typical hospital stay for an adult, during which a person is likely to stay in the same hospital bed for a period of several days, hospital stays for

babies in the NICU are rotated throughout a facility based on sensitive aspects of each patient's condition. For example, a patient may be on a warming table one day, in an incubator the next day, or in a bassinet on another day depending on his or her condition. This transitory nature of patient stays in the NICU requires robust identification. Moreover, it is very difficult to tell children apart during the nascent stages of their development. Gender is not apparent, and the babies do not have distinct facial characteristics. Finally, children often come to the NICU with identical or similar sounding surnames – according to one study, this factor alone is a distinct risk possibility approximately 51% of the time a NICU is in operation (Gray 2006).

Misidentification raises serious ethical and practical concerns. For example, Simpson et al. (2004) found that approximately 25% of the medication errors in a British NICU were associated with identification errors. In addition, Suresh et al (2004) found that 11% of errors reported to a voluntary error reporting system in Vermont were associated with patient errors. Once we know that a significant number of errors in the NICU are attributable to misidentification and we acknowledge that these errors pose harmful health consequences, this is a serious issue.

Despite the need for robust identification, the identification of babies in the NICU also must not be intrusive so as to infringe on the health of the infant. The skins of babies in the NICU, for example, are very sensitive to touch and to light. Therefore, any identification measure that makes physical contact with the skin needs to be used with caution – along those lines, identification methods should not force the doctor or nurse to need to physically move the patient, since this movement may do physical damage to the child. It may also interrupt the patient's *stasis* – studies have shown that the conditions in the NICU should simulate conditions

in the mother's womb as much as possible, and any exogenous forces that force movement may inhibit the child's normal development.

When visiting a NICU at Beth Israel, we were told that patient identification numbers were assigned sequentially. While this is an easy method of assignment, studies of medical error indicate that many common identification errors in medical records stem from flipped digits or the fact that a single digit may be off by one or two numbers. As such, numbering children sequentially in the NICU may be a risky proposition, especially when a set of triplets in the NICU – already practically indistinguishable – receives such sequential numbers. Moreover, there is no checkdigit at the end of patient identification numbers that are given out at Beth Israel Deaconness and other hospitals. Thus, there is no way to independently verify that the number corresponding to a given patient is legit (Gray et al. 2006).

Besides identifying the neonates themselves, identifying key NICU items such as breast milk is critical. This is because, when babies stay in the NICU, they are commonly separated from their mothers. The emphasis on identifying breast milk results from past problems that were caused by giving breast milk from an incorrect mother to an infant. Things that contribute to these errors, Gray notes, are incorrectly labeled specimens, difficult-to-read handwritten specimen labels, errors in verification of patient/aliquot identification, and systematic problems with the storage of the aliquots. These facts, combined with the reality that over 40,000 breast milk feeds are given in the average NICU each year, make it unsurprising that breast milk errors are frequent and of concern. \

Another issue of misidentification in the NICU relates to the aforementioned used of wristbands. A study by Howanitz et al. (2002) that surveyed over 200 hospitals found that roughly 7% of patients face identification problems resulting from wristbands – of these errors,

71% of them were a result of missing wristbands and the other 29% resulted from incorrect, missing, or incomplete information associated with those bands. Note that this 7% number reflects the rate of misidentification from wristbands of *general patient cohorts.* In the cohort of NICU patients, this rate may be much higher due to the aforementioned concerns of lacerating the sensitive skins of infants and the general difficulty of finding a suitable attachment point for the wristband on the infant. This means that many bands are affixed to patients' charts or incubators and that could lead to even more misidentification.

There are several potential benefits to applying RFID to this area. However, there is once again a substantial amount of uncertainty since babies within NICUs have never actually been tagged – this makes our utilitarian framework difficult to apply, since individuals who are subjected to the technology will not be able to make rational choices about its use. What we do know is that, if the benefits conferred unto infants are worthwhile, systems must be designed with particular care in this area. Some bodies of research speculate that RFID may present adverse health risks to individuals. The general nature of neonates may make them particularly susceptible to these risks. Thus, if an implementation of RFID were to exist in the NICU, its existence and implications should be fully explained to parents who should then be given the option (on behalf of the patient) to use a wristband that does or does not include RFID. While the tagging of breast milk can be addressed by taking measures similar to those we suggest for blood bags, NICU RFID implementations raise far more complex issues that will need to be addressed as they arise.

3. Care for the Elderly – Long Term Care Centers

Another interesting application of RFID that has been considered is within the realm of long-term care centers for the elderly. In long-term care centers, elderly patients may experience

symptoms of dementia or Alzheimer's disease, and this may result in their wandering away from the point of care. Although there are generally safeguards in long-term care centers to prevent such "escapes," these safeguards only extend to the care wards themselves – it may useful to employ a technology that can be applied when, for example, dementia patients are taken away from the facility by family or friends – however, measures are already in place in most long-term care centers to address that problem, so the real benefit of RFID is unlikely to come there.

Nevertheless, if RFID could adequately monitor the elderly population more generally, this may reduce the need for some long-term care centers in the first place. Given the impending baby boom and the demand that the rapidly growing elderly community will place on limited health care resources, hospitals could shift resources away from long-term care and towards broader applications in the home or elsewhere. Because long-term care is currently very resource intensive and often mandates that patients be separated from their families, this may be a good reason to apply RFID to patients who are experiencing such symptoms.

Most of the RFID solutions that have been proposed to facilitate long term care in the home focus on the ability to do "OKness" checking. A tagged elderly person lives in a home in which almost all items are tagged – prescription drugs, the telephone, and maybe even the TV remote control would be tagged in such scenarios. A close relative can then verify that the elderly patient takes his or her medicine at the prescribed time, and that other portions of the patient's "daily routine" are executed normally. If the patient diverts from his or her usual routine, the RFID system could be configured to set off an alarm that would notify a relative, nurse, or doctor. In addition, assuming that the patient was tagged, long periods of patient activity could be flagged by the system. For patients who are largely capable of living on their own, but are experiencing the initial signs of dementia or Alzheimer's, an RFID system may

provide the elderly patient with an alternative to living in a nursing home that would probably be much more desirable (Fishkin and Lundell, 2006).

Despite these benefits, we believe that such a system could raise several privacy issues. If RFID systems, for example, contained readers that are able to read tags throughout the entirety of homes, the systems would have to be designed so that the tags placed throughout the home were unreadable. We would not want an adversary sitting in the bushes outside a tagged patient's house to be able to track the rich elderly patient's every move. Maybe the tagged patient in this case has a substantial store of money in the house or other valuables, and this adversary could use the RFID system to gauge the likelihood of a successful burglary. Moreover, the system needs to be designed so that the readers cannot successfully read the tags from outside the home where the system is implemented. If we were in a world where adjacent houses employed these systems, we would not want two separate systems to be able to identify patients and items outside of their domain.

Additionally, the opt-in default for a system like this would, in many cases, not be exercised by the patients themselves. Because of this, relatives who make decisions for elderly patients need to be fully informed about the technology, just as mothers do when they are presented with the possibility that their babies are tagged with RFID. Serious ethical debates are raised when relatives try to make decisions "on behalf of" elderly or incapacitated patients, however, so it may be necessary to gauge public response to this form of RFID before implementing it. Finally, while such systems may be useful and indeed necessary, it is important to reaffirm the importance of personal interaction in taking care of the elderly. If implemented, RFID should not be used solely to give relatives "peace of mind" and excuse to not check up on or take care of their relatives.

4. Emergency Room and Operating Room RFID

Obviously, the opt-in provisions have their limitations, as we have stressed how these provisions break down when there is a lack of full information. *Spychips,* moreover, makes a valid point when it questions how legitimate consent actually is in the context of a hospital emergency room. In that context, people want to obtain care immediately and they will sign just about anything. It may have been somewhat unethical, therefore, for the Memphis Regional Medical Center to have conducted RFID trials in their operating room in which they claimed to obtain "consent" (Albrecht and McIntyre, 2005, p. 111). That is not to say that there is no room for legitimate ways to obtain an individual's consent in this area. Knowing that initial consent may not be legitimate, the hospital can later follow up with a patient to ensure that there is a willingness to be tagged. If efficiency gains within the ER and OR are significant – especially given the need for rapid service in this area – it may be worth relaxing opt-out provisions for these patients.

Empirically, however, RFID can promote tangible benefits in emergency department. Because every second counts in the emergency room, the efficiency gains from RFID in this area may have an even greater impact on patient health. At the emergency department at Christina Care in Wilmington, Delaware, for example, an RFID tracking system "was able to reduce the average length of stay for admitted patients by 36 minutes in the [emergency] department and to reduce the average length of stay for patient[s] released from the [emergency department] by 14 minutes" (Banks et al., 2007, p. 315). But it is not clear if this implementation has sought to protect privacy.

There are some final concerns that are raised by RFID applications in the ER and OR. For many patients, the ER is the only option for medical care. The poor oftentimes do not have

insurance and are unable to make everyday appointments with doctors at hospitals, meaning that these patients disproportionately seek the ER. In addition, any patient facing an emergency must always go to the ER. Because of this, many patients who are subjected to the ER do not have any choice in the first place. Thus, if an RFID enabled ER exists in a hospital, and all patients are required to be tagged in that ER, there are many patients who could effectively have no choice. And, while patients may obtain increased health benefits from an RFID enabled ER or OR, they should be given the option to opt-out wherever possible, and, most importantly, every effort should be made to ensure that care provided to those who opt-out is of comparable quality to the care given to those who do not opt-out. We believe this is possible in the context of an RFID enabled OR or ER. If an OR is enabled to use RFID tools and instruments, and much of the efficiency gains are realized from the tagging of these items, failing to tag the patient alone shouldn't substantially impact patient care. If it would impact patient care, and substantially more utility is gained from the necessary tagging of the patient, it may be a worthwhile consideration to relax opt-out provisions.

V. Conclusions and Recommendations

Privacy is a legitimate concern raised by RFID, and this paper has highlighted several areas where hospital RFID implementations may negatively impact patient privacy. Nevertheless, RFID also has the potential to increase operating efficiency, improve quality of care, and reduce medical error.

If we knew how significant the benefits of implementing RFID really were, we would be in a better position to assess the tradeoffs between privacy and the public good to determine an "ideal" policy. Unfortunately, we do not. Although asset management RFID pilots have indicated that significant ROI benefits can be realized within some hospitals, the realization of

positive ROIs in other hospitals is uncertain. And, although RFID has increased operating efficiency in some hospital pilots, the extent of RFID's positive impact remains blurry. Thus, additional pilots need to be undertaken within hospitals to assess how beneficial RFID really is. Ideally, such pilots will be designed in ways that will allow us to grasp the maximum benefits RFID confers.

Meanwhile, as we continue to assess the viability of RFID in the hospital setting, implementers of RFID should not do so hastily. Hospitals should be held accountable for infringements of patient privacy, and this accountability should extend to the technical design choices that are made by implementers.

After gaining a better understanding of the costs and benefits RFID provides in various hospital applications, we will be better able to assess privacy tradeoffs and make clear-cut recommendations. For example, in situations where time is of the essence, such as when patients are rushed to the ER, it may be worth relaxing opt-out provisions if that makes the difference between life and death. In other situations where RFID does not make as direct of an impact on an individual patient's health, hospital efficiency may be inhibited somewhat by additional bureaucratic red tape that serves the interest of privacy.

Meanwhile, there needs to be an acknowledgment that RFID is here to stay. In a survey of over 300 healthcare providers released in November 2005, roughly 74% of them anticipated investment in RFID by 2007. The FDA also continues to affirm its recommendation made in February 2004 that the entire pharmaceutical supply chain use RFID. And, most recently, the 2010 RFID Journal Live conference featured an entire track devoted to applications of RFID in the health care and pharmaceutical industries. At this conference, speakers were slated to discuss issues related to both pharmaceutical tracking and asset management.

The goal of this paper is to begin an interesting discourse on this provocative topic. It provides several recommendations that should be taken into account by all parties who are concerned about this technology. The literature reveals evidence both for and against RFID hospital implementations, and this raises more questions than answers. There is still much to learn in the emerging field of hospital RFID privacy, and future research will seek to empirically assess the adequacy of privacy protections in future RFID hospital implementations. Further, such research will attempt to accurately gauge hospital patients' true preferences in this area.

Appendix: Summary of Recommendations

Procedural Recommendations
1. Patients need to have the ability to make fully informed, rational choices as to whether or not they wish to participate in RFID pilots and implementations within hospitals
2. Implementers should not be allowed to assume that acceptance of RFID technology by patients in some areas implies acceptance in other areas.
3. Implementers need to ensure that systems conform to design principles that minimize privacy risks. Procedural privacy safeguards should complement these system designs.
4. Strong limits of information transfer should be observed, and patients should both know and have control over data that is associated with RFID tags. Even if tags themselves do not store information and personal information is stored on isolated databases, implementers need to consider insider abuse and all potential opportunities that personally identifiable information can be seen by unauthorized persons.
5. The opt-in default should be strongly observed because it promotes the dissemination of information to patients and allows them to make rational choices. The principle of full information underlies much of our analysis, and we believe that providing patients and the community full information leads to levels of public scrutiny that are necessary to ensure that RFID systems are protecting privacy in the public's interest. When patients do not opt-in, hospitals should offer bifurcated solutions.
6. The right of exit should also be strongly observed.
7. A framework should be created that allows patients to seek compensatory damages in the event their protected information is leaked or disseminated unjustifiably. Our utilitarian discourse requires this, and it is in the best interest of patients to have recourse against delinquent implementations.
Legal Recommendations
1. Institutions should be created that protect data privacy. Such institutions should have staff members that specialize in RFID privacy issues. This could take the form of a "Data Protection Commission" or some other form. These institutions could enforce RFID system design standards that minimize privacy risks and outline protocol that should be followed by hospitals and other health organizations that implement RFID solutions.
2. Laws should bolster HIPAA and existing laws to protect RFID privacy rights, but not in ways that are overly restrictive on the development of RFID applications. For example, laws should focus on scrutinizing the ways RFID systems are implemented, not on the fact that RFID is used in general.
3. The law has a role in ensuring that full information is provided. Patients, doctors, and the community will need to understand the motivation for passing laws. It is possible that patients, doctors, and the community at large will not take laws seriously if they do not understand the rationale for them. Laws need to have legitimacy to be effective, and legislatures need to give any laws that are passed legitimacy by communicating these rationales to their constituents and to doctors.
4. Lobbying should be regulated. Patients need to understand the nuances of the debate because corporations have substantial lobbying power. Corporate and lobbyist considerations should not outweigh *actual* constituent concerns. Legitimate proxies for public opinion need to be assessed before inaccurately assuming what the public believes based on the overrepresentation of some concentrated interest

References

Albrecht, K., & McIntyre, L. (2005). *Spychips: How Major Corporations and Government Plan to Track Your Every Move with RFID.* Nelson Current Publishers.

Banks, J., Pachano, M., Thompson, L., Hanny, D. (2007). *RFID Applied*. Hoboken, NJ: John Wiley & Sons.

Brewin, B. (2004, Nov. 15). RFID Gets FDA Push. *Federal Computer Week*. Retrieved April 24, 2010, from http://fcw.com/articles/2004/11/14/rfid-gets-fda-push.aspx.

Brown, Dennis E. (2007). *RFID Implementation*. New York, NY: McGraw-Hill.

Bruening, P. J. (Center For Democracy and Technology) (2004, July). *RFID Technology: What the Future Holds for Commerce, Security, and the Consumer*. Testimony Before the Subcomm. On Commerce, Trade, and Consumer Prot. of the House Comm. On Energy and Commerce, Washington DC, Retrieved April 24, 2010, from http://cdt.info/testimony/20040714bruening.pdf.

Cisco, Inc. (2003). Wireless LAN Benefits Study, Retrieved April 24, 2010, from http://newsroom.cisco.com/dlls/2003_NOP_WLAN_Benefits_Study.pdf

Collins, J. (2004). Hospitals Get Healthy Dose of RFID. *RFID Journal*, Retrieved April 24, 2010, from http://www.rfidjournal.com/article/view/920.

Dalton, J., Ippolito, C., Poncet, I., & Rossini, S. (2005). *Using RFID Technologies to Reduce Blood Transfusion Errors*. White Paper by Intel Corporation, Autentica, Cisco Systems, and San Raffaele Hospital. Retrieved April 24, 2010, from http://www.cisco.com/web/IT/local_offices/case_history/rfid_in_blood_transfusions_final.pdf.

DeNoon, D. (2005, July 27). Chip Implants: Better Care or Privacy Scare? *WebMD Medical News*, Retrieved April 24, 2010, from http://www.webmd.com/healthy-aging/news/20050727/chip-implants-better-care-privacy-scare.

Fanberg., H. (2004). The RFID Revolution. *Marketing Health Services,* 24(3), 43-4.

Federal Radio Frequency Device Regulations, 47 C.F.R. § 15.240.

Federal Trade Commission (2005, March). *Radio Frequency Identification: Applications and Implications for Consumers*, A Workshop Report from the Staff of the Federal Trade Commission, Retrieved April 24, 2010, from http://www.ftc.gov/os/2005/03/050308rfidrpt.pdf.

Fishkin, K., & Lundell., J. (2006). RFID in Healthcare. Simpson Garfinkel & Beth Rosenberg (Eds.). *RFID: Applications, Security, and Privacy*, Addison-Wesley.

Flaherty, D. H. (1989). *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, France, Canada, and the United States.* University of North Carolina Press.

Garfinkel, S., DeAlmo, J., Leng, S., McAfee, P., & Puddington, J.P. (2006). RFID In The Pharmacy: Q&A With CVS. Simpson Garfinkel & Beth Rosenberg (Eds.). *RFID: Applications, Security, and Privacy*, Addison-Wesley.

Goth, G. (2006). Tuning in to RFID. *Healthcare Informatics*. Retrieved April 24, 2010, from http://www.healthcare-informatics.com/ME2/dirmod.asp?sid=&nm=&type=Publishing&mod=Publications::Article&mid=8F3A7027421841978F18BE895F87F791&tier=4&id=B02C8A8740984CD7A7FDA241D324FAC1.

Gray, J.E., Suresh, G., et al. (2006). Patient Misidentification in the Neonatal Intensive Care Unit: Quantification of Risk. *Pediatrics*, 117(1), pp. 43-47.

HIPAA Privacy Rule, 45 C.F.R. § 164.512 (2009).

HIPAA Privacy Rule. 45 C.F.R § 160.103 (2009).

HIPAA Privacy Rule. 45 C.F.R. § 164.502(a) (2009).

HIPAA Privacy Rule. 45 C.F.R. § 164.502(a)-(b) (2009).

HIPAA Privacy Rule. 45 C.F.R. § 164.514(b) (2009).

Howanitz P.J., Renner S.W., & Walsh M.K. (2002). Continuous Wristband Monitoring over 2 Years Decreases Identification Errors: A College of American Pathologists Q-Tracks Study. *Archives of Pathology & Laboratory Medicine*. 126(7), 809-15,

Janz, B. D., Pitts, M.G., and Otondo, R. F. (2005). Information Systems and Health Care II: Back to the Future with RFID: Lessons Learned – Some Old, Some New. *Communication of the Association for Information Systems*, 15(1), 132-148.

Jaques, R. (2004). Hospitals Reluctant to Deploy RFID. *Computing*. Retrieved April 24, 2010, from http://www.computing.co.uk/vnunet/news/2124641/hospitals-reluctant-deploy-rfid.

Meyer, R. J. (2006). Why We Under-Prepare for Hazards. Ronald J. Daniels et al. (Eds.), *On Risk and Disaster: Lessons from Hurricane Katrina* (pp. 153-174). University of Pennsylvania Press.

Mich. Comp. Laws § 28.304 (2009).

Mobile Aspects (2005, Feb. 9). *University of Chicago Comer Children's Hospital Selects Mobile Aspects: RFID Solutions Deliver a Higher Quality of Patient Care, Safety, and Operational Efficiency* [Press Release]. Retrieved from http://www.mobileaspects.com/news_media/pressrelease/press_release_02.09.2005_University_of_Chicago.pdf.

Monegain, B. (2005, Sept. 12). Study: Passive RFID Not Ready for Prime Time in Healthcare. *Healthcare IT News*. Retrieved April 24, 2010, from http://www.healthcareitnews.com/news/study-passive-rfid-not-ready-prime-time-healthcare.

National Conference of State Legislatures (2010, January). State Statutes Relating to Radio Frequency Identification (RFID) and Privacy, Retrieved April 24, 2010, from http://www.ncsl.org/default.aspx?tabid=13442.

Nev. Rev. Stat. §§ 205.461-205.4675 (2009).

New Hampshire Commission on the Use of Radio Frequency Technology (2008, November). *Final Report*. Retrieved April 24, 2010, from http://www.gencourt.state.nh.us/statstudcomm/reports/1812.pdf.

RFID Journal (2010). *RFID Journal Live! Conference Brochure*, Retrieved April 24, 2010, from http://www.rfidjournalevents.com/live/live2010_brochure.pdf.

Rotenberg, M. (1994, October). *Privacy and Security for Medical Information Systems.* Presented at American Health Information Management AssociationNational Convention.

Schwartz, P. M. (2004). Property, Privacy, and Personal Data. *Harvard Law Review*, 117, p. 2055.

Schwartz, P. M. (2006). Privacy Inalienability and Personal Data Chips. Katherine Strandburg et al. (Eds.), *Privacy and Technologies of Identity: A Cross-Disciplinary Conversation* (pp. 93-114). New York, NY: Springer.

Schwartz, P.M. (2009). Preemption and Privacy. *Yale Law Journal*, 118, p. 902.

Siegal, G., Siegal, N., & Weisman, Y. (2001). Physicians' Attitudes toward Patients' Rights Legislation. *Medicine and Law*, 20(1), pp. 63-78.

Simpson, H.S., Lynch, R., Grant, J., & Alroomi, L (2004). Reducing Medication Errors Within the Neonatal Intensive Care Unit. *Archives of Disease in Childhood: Fetal Neonatal Edition* , 89(6), pp. F480-F482.

Slutsman, J., Kass, N., McGready, J. & Wynia, M. (2005). Health Information, The HIPAA Privacy Rule, and Health Care: What do Physicians Think? *Health Affairs*, 24(3), 832-841.

Solove, D. (2008). *Understanding Privacy.* Cambridge, MA: Harvard University Press.

Sommer, Kyle. (2009). Riding the Wave: The Uncertain Future of RFID Legislation. *Journal of Legislation*, 35, p. 48.

Sotto, L.J. (2005). An RFID Code of Conduct. *RFID Journal*. Retrieved April 24, 2010, from http://www.rfidjournal.com/article/view/1624/.

Stein, R. (2006, Mar. 15). Use of Implanted Patient-Data Chips Stirs Debate on Medicine vs. Privacy. *Washington Post*. Retrieved April 24, 2010, from http://www.washingtonpost.com/wp-dyn/content/article/2006/03/14/AR2006031402039.html.

Strickland, L. S., & Hunt, L. E. (2005). Technology, Security, and Individual Privacy: New Tools, New Threats, and New Public Perceptions. *Journal of the American Society for Information Science and Technology*, 56(3), pp. 221-234.

Suresh, G., Horbar J. D., Plsek, P., et al. (2004). Voluntary Anonymous Reporting of Medical Errors for Neonatal Intensive Care. *Pediatrics*, 113(6), pp. 1609-1618.

Sweeney, L. (1998). *Re-Identification of De-Identified Medical Data.* Testimony before the National Center for Vital Health Statistics, on the subject of medical data and privacy (HIPAA), Baltimore, MD.

Ulatowski, L.M. (2008). Recent Development in RFID Technology: Weighing Technology Against Potential Privacy Concerns. *Journal of Law and Policy For The Information Society*, 3, p. 623.

US Department of Health and Human Services (2003, May). *OCR Privacy Brief: Summary of the HIPAA Privacy Rule*, Retrieved April 24, 2010, from http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf.

VeriChip (2006). *VeriMed Patient Identification*. Retreived April 24, 2010, from http://www.verimedinfo.com/files/Patient_VM-003R2(web).pdf.

VeriChip (2006, March 20). *VeriChip Corporation Expands Infrastructure Rollout of VeriMed Patient Identification System – 172 New Physicians Elect to Offer VeriMed ID System to Patients* [Press Release]. Retrieved from http://www.redorbit.com/news/health/435457/verichip_corporation_expands_infrastructure_rollout_of_verimed_patient_identification_system/.

Wang, S., Chen, W., Ong, C., Liu, L., & Chuang, Y. (2006). RFID Applications in Hospitals: A Case Study on a Demonstration RFID Project in a Taiwan Hospital. *Proceedings of the 39th Hawaii International Conference on System Sciences*, 2006.