Chapter 10
Radio Frequency Identification in Hospitals: Balancing Hospital Efficiency and Patient Privacy

Christopher A. Suarez
Yale Law School, USA

ABSTRACT

Radio Frequency Identification (RFID) technology has been applied increasingly within the hospital setting. This chapter 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 RFID 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) technology 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
Radio Frequency Identification in Hospitals

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 chapter, 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 can be designed to 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, therefore, 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 the technology 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 be 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 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 transmit data. While these technical choices are beyond the scope of this analysis, all of them have a direct bearing on the privacy implications of the technology.

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 to society. Further, the ultimate form of many RFID implementations in hospitals remains unseen. While many hospital RFID applications have been proposed and implemented, future applications may alter the balance of considerations made in this analysis. By addressing a wide variety of hospital RFID applications, I hope to address the 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. I also use the literature to confirm that the principles are consistent with those established by well-known privacy advocacy groups and 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. In Part IV, I 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.