

An RFID Code of Conduct

Existing laws protect the privacy of patients' medical information. But an additional layer of protection is needed before RFID technology becomes accepted in the health-care arena.

May 30, 2005—The use of RFID technology in the healthcare arena holds enormous promise. It could lead to greater accuracy and efficiency in treating patients by making medical information immediately accessible to healthcare providers. But privacy concerns present a significant obstacle to its widespread acceptance. Given the sensitivity of personal medical data, patient confidence in the integrity of RFID technology is essential. Until patients' privacy concerns are allayed, the use of RFID in healthcare could be a difficult sell.

One of the most pressing privacy concerns is the inappropriate collection of health information through RFID technology. The concern stems from the problem of the surreptitious collection of data with RFID tags in other settings. In libraries, for example, RFID tags could be attached to books without the borrowers' knowledge and collect certain data without their consent.

In healthcare, the inappropriate collection of information is a less significant concern, because patients consent in advance to the use of RFID devices such as the VeriChip, which is imbedded under a person's skin. Furthermore, little data are stored in the VeriChip itself; even if it were secretly scanned, the VeriChip would only disclose a 16-digit identification number. That ID number is meaningful only to providers who can use it to gain access to the patient's medical data through a Web-based application.

The main concern, then, is unauthorized access to the database. But unauthorized access is a problem that other entities—banks and credit bureaus, for example—contend with all the time. Any database in which health information is maintained would have to be protected by similar policies and technologies to guard against unauthorized access.

Another concern is the unauthorized alteration of patients' medical data by those who have access to it, including healthcare providers and employees who work with the company providing the RFID services. In any situation in which data integrity is an issue, authentication technologies and other safeguards must be used to help ensure that only those who are authorized to amend the data may do so.

In addition, there is the potential for intentional misuse or unauthorized disclosure of the data by the authorized data holder. While this is a legitimate and significant concern, it is not unique to the RFID context. It is an issue we confront daily in connection with the collection and maintenance of data sets. Whether information is recorded on paper or electronically, guarding against its misuse or unauthorized disclosure is a security and organizational oversight issue that must be addressed by every entity that is entrusted with personally identifiable information.

The good news is that while RFID technology is new, the privacy concerns surrounding it are not. As a result, several time-tested remedies addressing the concerns exist in other contexts.

On the statutory front, the privacy and security regulations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and a host of other federal and state laws provide privacy protections. In

addition, the Fair Information Practices devised by the Federal Trade Commission provide a blueprint for an industry code of conduct.

HIPAA's Privacy and Security Rules impose strict limits on the use and disclosure of health information. HIPAA applies to all health information collected in any form or fashion by healthcare providers, health plans and healthcare clearinghouses (entities). As a result, patients associated with entities covered by HIPAA already have potent privacy protections in place.

Other existing laws govern those entities that are not covered by HIPAA. For example, the unauthorized use or disclosure of medical data may be a violation of Section 5 of the Federal Trade Commission Act and its state counterparts, which prohibit entities from engaging in unfair or deceptive trade practices. In fact, the FTC has availed itself of Section 5 in cracking down on privacy and information security abuses in numerous instances. In addition, with respect to unauthorized data users who illicitly intercept and exploit medical information obtained through an RFID network, existing laws provide the necessary tools to actively combat and deter this illegal behavior.

To offer an additional layer of protection, the healthcare industry should consider a code of conduct for entities that maintain or permit access to medical data associated with an RFID network. The Fair Information Practice principles and HIPAA's Privacy and Security Rules offer excellent guidance in developing such a code. Ideally, the code would include the following:

- *A notice provision.* Patients who are "chipped" would receive a plainly written notice of the data holder's information practices. Satisfactory notices would clearly identify, for example, the types of data collected, the uses of the data and the security measures in place to protect the data.
- *A consent provision.* Data holders generally would use and disclose health data in a manner to which the patient has explicitly consented.
- *The ability to amend data.* Patients would be able to review their RFID-related health information, challenge its accuracy and, if necessary, correct it.
- *Assurance of data integrity and security.* The code would establish minimum standards to protect against the loss and the unauthorized alteration, secure destruction, access, use and disclosure of data.
- *Instruction on data retention and chip deactivation.* The code would clearly instruct patients how to deactivate an RFID chip and how to request the destruction of medical data maintained in an RFID chip or RFID-related database.
- *Reliable accountability and enforcement.* The code would establish strict accountability standards, enforcement provisions and redress mechanisms for parties participating in an RFID system.

Given the sensitivity of personal medical information, privacy advocates are justifiably concerned about the use of RFID technology. While existing laws are available to address the potential harms, RFID stakeholders should work together to develop and adopt an industry code of conduct to further protect against harms that might result from the misuse of data. A coordinated approach by all stakeholders would provide the public with the confidence needed to support the advancement of this beneficial technology.

Lisa J. Sotto is a partner at Hunton & Williams and head of the law firm's Regulatory Privacy and Information Management practice. She was recently appointed as vice chair of the Data Privacy and Integrity Advisory Committee of the U.S. Department of Homeland Security. To comment on this article, click on the link below.