

REPORT OF THE COUNCIL ON ETHICAL AND JUDICIAL AFFAIRS\*

CEJA Report 5-A-07

Subject: Radio Frequency ID Devices in Humans  
Presented by: Robert M. Sade, MD, Chair  
Referred to: Reference Committee on Amendments to Constitution and Bylaws  
(Richert E. Quinn, Jr., MD, Chair)

---

1 INTRODUCTION

2  
3 Radio frequency identification (RFID) tags are computer chips connected to miniature antennae  
4 that can be used to transmit information electronically via a proximate RFID reader. The use of  
5 these devices in health care represents another promising development in information technology,  
6 but also raises important ethical, legal and social issues. Specifically, the use of RFID labeling in  
7 humans for medical purposes may improve patient safety, but also may pose some physical risks,  
8 compromise patient privacy, or present other social hazards.

9  
10 This report responds to Resolution 6 (A-06), "RFID Labeling in Humans," which called for study  
11 of the medical and ethical implications of RFID chips in humans. This report focuses on ethical  
12 issues in the use of RFID chips, specifically in regard to their implantation for clinical purposes.

13  
14 BACKGROUND

15  
16 Radio frequency identification devices utilize wireless technology to communicate data via signals  
17 in the radio frequency range of the electromagnetic spectrum. Data are stored in a microchip  
18 attached to an antenna, and packaged so that they can be attached to or embedded in products,  
19 animals, or people.

20  
21 The two main types of RFID tags are passive and active. Passive tags contain no internal power  
22 supply. They convert the radio frequency energy emitted from a reader device into signals that  
23 transmit stored data for a distance of a few feet. These passive devices currently have restricted  
24 amounts of data storage and are of limited functionality, because the information they contain  
25 cannot be modified.

26  
27 In comparison, active RFID tags contain an internal battery, which provides increased reliability,  
28 longer transmission ranges, on-tag data processing and greater data storage.<sup>1</sup> While their capacity  
29 to process data internally allows for expanded capabilities in the future, their greater transmission  
30 range presents a more substantial threat to data confidentiality and patients' privacy.

31  

---

\* Reports of the Council on Ethical and Judicial Affairs are assigned to the reference committee on  
Constitution and Bylaws. They may be adopted, not adopted, or referred. A report may not be amended,  
except to clarify the meaning of the report and only with the concurrence of the Council.

1 In October 2004, the US Food and Drug Administration (FDA) approved the first RFID tags  
2 specifically intended for human implantation.<sup>2</sup> Approved RFID devices are currently limited to  
3 passive units, intended for identifying patients. Active RFID chips may be approved in the future.  
4

5 Human-implanted passive RFID devices that identify patients may also contain essential biometric  
6 and medical information. The tags are primarily intended for patients with chronic diseases, such  
7 as coronary artery disease, chronic obstructive pulmonary disease, diabetes mellitus, stroke or  
8 seizure disorder, or are implanted into patients with medical devices such as pacemakers, stents, or  
9 joint replacements. These devices are approximately the size of a grain of rice, and are implanted  
10 under the skin via a hypodermic-type needle in less than one minute.<sup>3</sup>  
11

## 12 INFORMATION SYSTEMS

13

14 RFID tags may promote the timely identification of patients and expedite access to their medical  
15 information. As a result, these devices can improve the continuity and coordination of care with  
16 resulting reduction in adverse drug events and other medical errors.<sup>4</sup>  
17

18 RFID tags also may improve efficiency within the health care system. In conjunction with  
19 improved medical record management, these devices may facilitate access to patient records,  
20 medication lists, and diagnostic tests.<sup>5</sup> To be maximally effective, however, the information in  
21 these devices must be adequately integrated into present clinical information and communications  
22 systems, laboratory databases, and pharmacy systems.<sup>1</sup>  
23

24 Appropriate processes also must be developed to inscribe, read and archive data stored on RFID  
25 tags. As new designs enter the marketplace, the emergence of competing standards may present  
26 problems for hospital staff if a patient's ID tag proves incompatible with the interrogation devices  
27 employed by the hospital.<sup>1</sup>  
28

## 29 PHYSICAL RISKS TO PATIENTS

30

31 These devices may present physical risks to the patient. Though they are removable, their small  
32 size allows them to migrate under the skin, making them potentially difficult to extract. However,  
33 this tendency may be minimized by constructing RFID tags from materials that permit surrounding  
34 tissue to encase the device. In addition, RFID tags may cause electromagnetic interference, which  
35 may interfere with electrosurgical devices and defibrillators.<sup>1</sup> Finally, it has not been determined  
36 whether RFID tags might affect the efficacy of pharmaceuticals.<sup>1,6</sup>  
37

## 38 PATIENT PRIVACY AND SECURITY

39

40 The primary concerns surrounding human RFID labeling pertain to their potential impact on patient  
41 privacy and security. Physicians must assure patients that their medical information will be held in  
42 confidence (see Opinion E-5.05, "Confidentiality"). Moreover, maintenance of privacy is required  
43 to protect patients from embarrassment, potential social discrimination, loss of health care  
44 coverage, or other detrimental consequences (see Opinion E-5.059, "Privacy in the Context of  
45 Health Care").  
46

47 At this time, the security of RFID devices has not been fully established. Physicians, therefore,  
48 cannot assure patients that the personal information contained on RFID tags will be appropriately

1 protected. In light of these security concerns, the FDA currently requires RFID transponders to  
2 store only a unique electronic identification code to be read by the scanner.<sup>2</sup> This identification  
3 code can then be used to access patient identity and corresponding health information stored in a  
4 database.

5  
6 To protect confidentiality and privacy, the medical community should advocate for the adoption of  
7 other protections, such as computer encryption or digital signatures. Ultimately, the medical  
8 community should undertake appropriate efforts to prevent unauthorized access to patients'  
9 information contained on RFID tags (see also E-5.07, "Confidentiality: Computers," AMA Policy  
10 Database).

#### 11 12 INFORMED CONSENT

13  
14 To properly respect patient autonomy, RFID tags should not be implanted or removed without the  
15 prior consent of patients or their surrogates (see E-8.08, "Informed Consent," and E-8.081,  
16 "Surrogate Decision Making"). During the consent process, decision-makers should be informed  
17 of the potential risks and benefits associated with RFID tags, including the many uncertainties  
18 regarding their efficacy. Patients are also entitled to know who will be granted access to the data  
19 contained on RFID tags and the purposes for which this information will be used.<sup>7</sup>

#### 20 21 FURTHER CONSIDERATIONS

22  
23 It seems likely that utilization of RFID devices for medical purposes will expand.<sup>4</sup> The medical  
24 profession must continue to monitor the efficacy of these devices. If RFID tags are proven to  
25 benefit patient care significantly, the profession should advocate for widespread adoption of RFID  
26 technology, and for policies that make RFID tags available to all patients who would benefit (see  
27 Opinion E-2.095, "The Provision of Adequate Health Care").

28  
29 However, if objective evidence demonstrates negative consequences that outweigh the benefits in  
30 relation to health care, the medical profession will bear an important responsibility to oppose the  
31 use of RFID labeling in humans.

32  
33 Finally, physicians should be aware of emerging non-medical applications of human-implantable  
34 RFID devices. For instance, active RFID technologies might be considered for the tracking or  
35 surveillance of individuals who pose a threat to others. Although this is only one of many possible  
36 uses of RFID technology in the future, it alerts the medical profession to the need for continuous  
37 assessment of the appropriate role of physicians participating in RFID labeling of human beings.  
38 Indeed, certain uses could constitute an infringement upon patients' individual liberties, placing  
39 physicians in a position to act as patient advocates by promoting the use of other, less intrusive  
40 alternatives, when available.<sup>4</sup>

#### 41 42 CONCLUSION

43  
44 RFID technology has the potential to improve patient care as well as patient safety. However, the  
45 safety and efficacy of human-implantable RFID devices has yet to be established. Therefore, the  
46 medical community should support further investigations to obtain the data necessary to make  
47 informed medical decisions regarding the use of these devices. The medical community should

1 also be sensitive to potential social consequences of RFID devices, such as non-medical  
2 applications in law enforcement.

3

4 RECOMMENDATION

5

6 The Council on Ethical and Judicial Affairs recommends that the following be adopted and the  
7 remainder of the report be filed.

8

9 Radio frequency identification (RFID) devices may help to identify patients, thereby improving  
10 the safety and efficiency of patient care, and may be used to enable secure access to patient  
11 clinical information. However, their efficacy and security have not been established.  
12 Therefore, physicians implanting such devices should take certain precautions:

13

14 (1) The informed consent process must include disclosure of medical uncertainties  
15 associated with these devices.

16

17 (2) Physicians should strive to protect patients' privacy by storing confidential  
18 information only on RFID devices with informational security similar to that required  
19 of medical records.

20

21 (3) Physicians should support research into the safety, efficacy, and potential non-medical  
22 uses of RFID devices in human beings.

23

24 (NEW HOD/CEJA Policy)

Fiscal Note: Staff cost estimated at less than \$500 to implement.

## REFERENCES

- <sup>1</sup> Ingeholm; Mun, K; Mun, SK. RFID in Healthcare: The Applications, and Obstacles, Are Many; *Journal of AHIMA*; 2006. 77(8): 56-62.
- <sup>2</sup> US Food and Drug Administration. Medical devices; general hospital and personal use devices; classification of implantable radiofrequency transponder system for patient information and health information. *Federal Register*. 2004; 69(237): 71702-4.
- <sup>3</sup> DeNoon D. Chip implants: Better care or privacy scare. 2005. Accessible at” <http://www.webmd.com/content/Article/109/109216.htm>
- <sup>4</sup> Wicks, AM; Visich, JK; Li, Suhong. Radio Frequency Identification Applications in Hospital Environments; *Hospital Topics*.2006; 84(3): 3-8.
- <sup>5</sup> VeriMed™ Information Center for Patients; <http://www.verimedinfo.com/content/intro/physicians>
- <sup>6</sup> Wasserman, Elizabeth. A Prescription for Pharmaceuticals; *RFID Journal*. 2006. Accessible at: <http://www.rfidjournal.com/magazine/article/1739/1/173/>
- <sup>7</sup> Opinion of the European Group on Ethics in Science and New Technologies to the European Commission, *Ethical Aspects of ICT Implants in the Human Body*. 2005.