Not a scalpel: RFID implants for patients and personnel in hospitals

Maria Bottis

The objective of ensuring efficacy in the delivery of healthcare has always been a legitimate aim for regulators and technologists alike[1]. It has long been thought that information health technology could aid in great cost savings and also, in the optimal addressing of the needs of patients. Electronic health records, clinical decision support and computerized physician order entry are among the information health technology applications that have been part of current information health technology in hospitals for quite some time.[2]

Technology, of course, is not a purpose in itself. It supposedly aims at serving people's existing and proven needs, in a way that while using technology (and paying its costs), we can justify the decision of creation and use of this technology not only because as humans we love to create and innovate, and as technologists we enthuse over new "gadgets", or even to make money in inventing new markets for our own pure financial gain, but because we address people's real needs and enhance their quality of life. Our research, then, should be worth both time and money, as otherwise it would not justify itself and time and money should be devoted to other endeavors.

In the context of healthcare, people become more vulnerable than in any other context[3] and their paramount needs, interests and rights dictate that we be even more careful in our technological inventions. Patients must be treated in the most careful way possible. Human rights are implicated in healthcare delivery in an acute manner and this is the reason why healthcare/medical ethics were amongst the first fields of ethics developed early in the 19th century. The distinct power play with the figure of the potent physician on one hand and the feeble child-like patient on the other must now be completed with a healthcare technologist

1. Paper presented at the Barcelona workshop of the Liss Working Group 4, in October 2011. The meeting took place at the International University of Catalunya, Spain. It was the sixth meeting of the working group 4 of Liss.
2. *Furukawa, M. F., Raghu, T. S., Spaulding, T. J., & Vinze, A.*, Health Affairs, 27, (3), 865-875 (2008).
3. See generally *Katz J.*, The Silent World of Doctor and Patient, 1983.

somewhere in the background, who in effect alters the picture often in very important ways. So, electronic health care information systems both offer new opportunities for monitoring access to health and impose additional challenges for protecting human rights[4]. The delivery of medicine is more and more dependant on technology, starting with the results of an endless series of medical diagnostic and other tests etc. We have also seen a gradual but steady distancing of a patient from her physician; the relationship often is not even a relationship at all, but an instant occurrence once in time.

RFID technology, that is radio frequency identification, is a rather new technology which was not initially relevant to health care. RFID uses radio waves in order to permit the instant identification of items, so data is possible to be processed over short distances[5]. RFID systems can identify objects which bear a RFID tag without line-of-sight contact and permit the wireless transmission of data and connection to databases and various applications. The identification of objects with certainty and at real time of course has been and is something we want to pursue in many domains. When we do our inventory, we know in an instant what items we have in stock.

In healthcare delivery services, we also have many objects to tag, and therefore secure their immediate and safe identification. This ranges from medical sponges and scalpels and other surgical instruments. One of the common lawsuits in medical negligence has been a surgical instrument negligently left in the body of a patient[6]. This is not the same, of course with the operation on the wrong person-the solution «tag a patient» as you "tag" a sponge appears immediately problematic. Patients with dementia or Alzheimer's disease could seem suitable for the use of a 'portable' identification system, especially in the case where a patient wanders around and caregivers may not easily find where she is. But as evident in the literature, the questions of using RFID technology on people, patients or healthcare personnel pose significant ethical questions, especially on privacy/data protection, justice/equity and more importantly, on the commodification of human beings (hence, dignity).

4. *Chapman A.,* Developing Health Information Systems Consistent with Human Rights Criteria, in *Chapman A.*, (ed.), Health Care and Information Ethics: Protecting Fundamental Human Rights, Sheed & Ward, 1997, p. 3.

5. *Bannon A.*, RFID: Radio Frequency Identification OR Real Frailty in Data Protection? JILT, http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2008_1bannon. Last access June 10, 2013.

6. Among the surgical instruments left in the body of patients are: artery forceps, surgical retractors, towel and tubing clamps, tissue and dressing forceps, needle holders, splinter forceps, surgical scissors, vascular forceps, nail nippers, blades etc.

1. RFID technology in healthcare

Any RFID infrastructure is composed by a a tag and a reader. The tag stores data and an antenna transmitting these data and the reader also has an antenna which receives the data and a demodulator, which translates the analogue information into digital data[7]. Tags can be classified as *passive* (where tags have no own power supply, receiving energy from the reader antenna) and *active* (where tags have their own power supply)[8]. Passive tags are inexpensive and very small and their life span is almost unlimited[9]. The passive tags store restricted amounts of data storage and are of limited functionality because the information they contain cannot be modified[10]. Active RFID tags permit expanded capabilities for the future, but their greater transmission range presents a more substantial threat to data confidentiality and patient's privacy[11].

RFID tags were not designed with the more efficient delivery of healthcare in mind; the main concern was to tag and identify objects for sale. They were the next generation of bad codes and the retail sector was one of the first to adopt this technology. With the tags, the retailer can control and lever the availability of products in a store and in storage. An unprecedented growth of sales took place in 2010 when the sale of passive EPC RFID tags took place and the sales volume exceeded one billion units[12]. Prices of tags are also decreasing, reaching $0,07 each[13]. As cheap as this may sound, we must not loose sight of the fact that the decision for a hospital to adopt RFID technology for either medical equipment or patients/personnel, or both, is definitely a very costly decision.

7. Article 29 Data Protection Working Party. Working document on data protection issues related to RFID technology. WP 105, January 19, 2005, p. 3, available at ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp105_en.pdf. Last access June 10, 2013.
8. See generally *Alexandropoulou T. & Mavrides J.*, RFID identification and data protection, Proceedings, E-democracy: challenges of the digital age, 2nd Conference, p. 445, available at http://scis.aua.gr/Praktika2_1_4.pdf (in Greek). Last access June 10, 2013.
9. *Reuven R. Levary*, et al, Radio Frequency Identification: Legal Aspects, 12 RICH. J.L. & TECH. 6 (2005), *at* http://law.richmond.edu/jolt/v12i2/article6.pdf. Last access June 10, 2013.
10. American Medical Association, Report of the Council on Ethical and Judicial Affairs, CEJA Report 5-1-07, Radio Frequency ID Devices in Humans, available at www.ama-assn.org/ama1/pub/upload/mm/467/ceja5a07.doc. Last access June 10, 2013.
11. Id, p. 1.
12. RFID journal, Sales of EPC RFID tags, ICsa increase reach record levels, available at http://www.rfidjournal.com/article/view/7952.
13. http://rfidjournal.com/faq/20. Last access June 10, 2013.

Hundred thousands or even millions of dollars[14] have been paid for the installation of RFID technology in hospitals. Additionally, the target market of VeriChip, the only US company authorized by the FDA to construct and sell 'medical' RFID chips reaches 45 million Americans[15]. Numbers of course increase when it comes to an international market.

Especially in healthcare, it is supported that generally, the use of RFID tags can boost asset utilization rates with real-time location systems (RTLS), leverage RTLS and RFID technologies to wring greater efficiencies out of existing resources, reduce medical errors by tracking medical devices, increase patient monitoring and safety and improve medication management[16]. RFID tags have been used initially in the pharmaceutical industry, to make tracking of medicines easier and prevent counterfeiting. The US FDA has issued guidelines for RFIDs on drugs packaging for tracking and against counterfeiting[17].

From the tracking of medicines, RFID technology has passed to the most sophisticated tagging of medical equipment, and also, people involved in any way in healthcare. People are now also tagged, at times: personnel and patients. The tagging ranges from a bracelet, a plastic badge that has buttons to be operated by the hospital or even an implant[18], into the person's body. In 2007, approximately 1.200 physicians and 66 hospitals had applied to try the VeriChip system, the RFID implantable device, assuming patients requested it for their safety, under informed consent procedures and databases support it, so as to be effective[19].

14. For example, the cost for three Virginia hospitals to use RFID for five years came up to 3,9 million dollars, see *Collins*, Hospitals Get Healthy Dose of RFID, http://www.rfidjournal.com/article/view/920/. Last access June 10, 2013.

15. *Lewan T.*, Chip Implants Linked to Animal Tumors, The Washington Post, http://www.hwshingtonpost.com/wp-dyn/content/article/2007/09/08/AR2007090800997_pf.html. Last access June 10, 2013.

16. RFID in healthcare, http://rfidjournalevents.com/healthcare/. Last access June 10, 2013.

17. Article 29 Data Protection Working Party, id.

18. The RFID implant was approved by the Food and Drug Administration for human use in 2004. A company named VeriChip was the approved by the FDA company to supply the implantable in humans RFID chip. When the chip is scanned, it reveals a code of 16 digits, which in its turn is the code for the patient's medical records held in a database.

19. *Kanellos M.*, Patients, doctors staying away from implantable RFID chips, CNET news, February 12, 2007.

The use of RFID tags in hospitals is expanding[20]; and 10-year growth projections reached in 2007 2 billion dollars[21].

I will offer some examples of hospitals that have adopted RFID technology in order to offer more efficient care in terms of cost, speed, safety e.tc. RFIDs have been embedded in patient bracelets so that the staff may electronically identify patients before surgery and avoid surgery upon the wrong patient. Patient RFID bracelets allow the medical staff to identify electronically a patient before surgery or before administering blood transfusions[22]. In emergency care, RFID is used to monitor and analyze patients' physical locations, as well as the status of their care, then display that information in charts and graphs via computers located throughout the department (case of the Albert Einstein Medical Center[23], implementation of the system took place in 2009).

Hospitals have also begun to use RFID technology with the goal to locate pieces of equipment[24] when medical staff needs them, so that nurses spend less time "hunting and gathering" equipment that they need and spend more time towards

20. *Wicks AM, Visich JK & Suhong J.*, Radio Frequency Identification Applications in Hospital Environments: Hospital Topics, 2006; 86(3) 3-8.

21. *Ashar BS & Ferriter A.*, Radiofrequency identification technology in healthcare: benefits and potential risks. JAMA 2007; 298(19): 2305-2307.

22. In one of the most famous "wrong patient" medical negligence cases, the physician mistook the five months pregnant claimant (Mrs. Thi-Nho Vo) for another woman, with a very similar name (Mrs. Thi Thanh Van Vo) and performed upon the claimant the medical procedure planned for the other patient. The result was the miscarriage of a five months old fetus. The case was heard by the European Court of Human Rights in 2004 (*Vo v. France*, No. 53924/00, 19 Eur. Ct. H.R. July 8, 2004, available at http://www.echr.coe.int.). Operating on the wrong side of the patient, on the wrong organ or on the wrong patient altogether –name similarities are seen in these cases- have been the subject of extensive research and has been well documented in the relevant medical negligence bibliography. See indicatively *Chassin MR & Becher EC*, The wrong patient, Ann. Inter. Med. 2022; 136;826-833, *Neily J., Mills PD & Eldridge N. et al.*, Incorrect surgical procedures inside and outside the operating room, Arch.Surg. 2009; 144: 1028-1034 and *Rhodes P., Giles SJ, Cook GA et al.*, Assessment of the implementation of a national patient safety alert to reduce wrong site surgery, Qual. Saf. Health Care 2008; 17; 409-415.

23. Philly Hospital Uses RTLS to Track Patient Flow, Care and Training, http://www.rfidjournal.com.

24. See for example the deal for the three Virginia hospitals mentioned above: in their case, the RFID network in each hospital will be able to determine the exact location of all tagged medical equipment and other mobile assets. The system will also show whether each item is in use, available or in need of servicing.

direct patient care[25]. Hospitals may also efficiently utilize the equipment they have and lower expenses on equipment rental and purchasing[26]. Hospitals have used this technology to locate where patients are and to collect data on patient movement throughout hospital services[27]. To simplify the "travel" of a patient in a hospital, she usually moves from admission, exams, care, recovery, discharge and billing[28]. In all these "stops", RFID technology can help in terms of cost efficiency and management[29], heightened patient safety, better tracking of supplies and real-time management of hospital assets[30].

Very recently, in 2011, a new special RFID technology was implemented allowing the monitoring of whether hospital personnel washes their hands, as obliged. Hospitals in this case will be able to create a record of hand-washing compliance and also send alerts to people when they attempt to see patients without washing their hands first. This way, it is expected that hospital-acquired infections will lessen[31].

---

25. *Fisher J.*, 2006, Indoor Positioning and Digital Management: Emerging Surveillance Regimes in Hospitals, in *T. Monahan* (ed.), Surveillance and Security: Technological Politics and Power in Everyday Life, pp. 77-88, New York: Routledge, at p. 80.

26. *Glabman M.,* Room for tracking. RFID technology finds the way, Mater. Manage. Health Care 13 (26–28) (2004) 6, 31–4.

27. *Fisher*, id., 80. Note 25.

28. As mapped in *Cangialosi A., Monaly J. & Yang S.*, Applying RFID to Patient Care: Challenges and Opportunities, available at www.irma-international.org/viewtitle/33248/.

29. Id. More particularly: "…Hospital workflow could be streamlined by: 1. Scanning information from a patient wristband directly into the hospital information system. Wristbands could contain information in human readable and other electronic forms (barcode) to work with other information systems in use. 2. Scanning and transmitting information about patient blood vials to the central data repository. Machine-printed labels, which are both human readable and RFID enabled, could be placed on the vials specifying the requested lab tests before samples are collected. 3. Working in reverse, the RFID scanner could obtain information from the central repository and display it using a more complex reader that comes with a graphical display. The display can provide information to verify the identity of a patient (such as the name of the patient and a photo) and the patient's previous lab work, as well as confirm that the requested lab tests have been performed with their time and location as the phlebotomist makes rounds. 4. Identifying discrepancies between the vials drawn and the vials actually sent to the lab for processing…". *Cangialosi A., Monaly J. & Yang S.*, Leveraging RFID in hospitals: Patient lie cycle and mobility perspectives, IEEE April 2007, Applications and Practice.

30. *Fisher*, id., 81. Note 25.

31. GOJO brings WiFi-based RFID to hand-washing dispensers, RFID journal, 22.2.2011, http://www.rfidjournal.com/article/view/8234.

2. Privacy implications of RFID implants

Perhaps an easy-and legitimate- criticism of the RFID implantable (and other) chips is dangers to privacy of a patient[32]. Indeed, scholarly attention to these devices has primarily come from the fields of bioethics and information ethics and form privacy advocates[33]. In a European setting, the Directives[34] on data protection dictate that the informed consent is the default rule when it comes to personal data processing, as in the case of RFID medical implants and so, the first "lens" one should explore the chip field is the privacy lens[35].

32. "…The primary concerns surrounding human RFID labeling pertain to their potential impact on patient privacy and security. Physicians must assure patients that their medical information will be held in confidence. Moreover, maintenance of privacy is required to protect patients from embarrassment, potential social discrimination, loss of health care coverage and other detrimental consequences…: American Medical Association, Report of the Council on Ethical and Judicial Affairs, CEJA Report 5-A-07, available at http://epic.org/privacy/rfid/ama-report.pdf. Accessed June 10, 2013. But see also the statements of Arthrur Caplan, Director of the Center for Bioethics at the University of Pennsylvania in DeNoon, Chip Implants: Better Care of Privacy Scare? WebMD Health News, http://webmd.com/healthy-aging/news/20050727/, "…you are more likely to die or be harmed by lack of medical information…in an emergency it is important for doctors to know what your allergies and medical problems are, who your relatives re and how to reach them, your blood type and so on…if a chip could also serve as a GPS reporting my location, or act as an emergency transponder, I would definitely upgrade…". Last access June 10, 2013.

33. *Monahan T. & Fisher J.*, Implanting inequality empirical evidence of social and ethical risks of implantable readio-frequency identification (RFID) devices, International Journal of Technology Assessment in Health Care, 26:4 (2010), 370-376, at 371.

34. I refer mainly to the Directive 1995/46 (main data protection Directive) and the Directive 2002/58 on privacy in electronic communications, which also applies to RFID systems.

35. Especially on RFID and privacy, in 12.1.2011 the Data Protection Working Party 29 endorsed the Privacy and Data Protection Impact Assessment Framework for RFID Applications of 12.1.2011, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_annex_en.pdf. Last access June 10, 2013. The Working Party stated that the Privacy and Data Protection Impact Assessment accepted (after a revision) promotes privacy by design, better information to individuals and transparency and dialogue with competent authorities. Id. The discussion in Europe on RFID implants is mainly centred on the privacy and data protection question. See also the Commission Recommendation (2009) On the implementation of privacy and data protection principles in applications supported by radio-frequency identification, C (2009), 3200 final.

In this sense, we should point that the chip is not encrypted and therefore, not secure[36] and that it could be cloned. A cloned chip could offer access to a patient's medical record and/or access to her health insurance. To implant people only after their informed consent has been obtained under the known rules of medical law and ethics and following the standards does not, of course, rule out the possibility of medical identity theft. It should be also noted that, when it comes to tags, it is supported that RFID "…is fundamentally secure because tags are extremely difficult to counterfeit and impossible to read without a reader..." and so it is supported that tags are physically tamper-proof[37]. It is also supported that personal health information is not at risk., if RFID tags carry only a unique ID that requires an external systems database to match to patient demographics and most tags would be removed at discharge[38]. The US FDA requires that RFID transponders store only a unique electronic identification code to be read by the scanner[39]. And the AMA Ethics Code for RFID chip implants recommends that the storage of confidential information in a chip implant utilizing informational security similar to that required for medical records[40].

On the other hand, people have the right to risk the rare event of an identity theft of this sort, or a loss of privacy more generally-they can prefer to be implanted with a chip for their own good[41]. In this sense, patients who consent to the use of the RFID implants under the standards of informed consent are deemed to be free to opt for the implant/RFID device. People with epilepsy, heart disease or mental impairment may indeed benefit from a RFID implant, as these people may not always be able to effectively communicate with healthcare workers and

36. *Karr*, id., See also Report, as above, note 32 page 2 ("…at this time, the security of RFID devices has not been fully established…").

37. *Finkenzeller K.*, RFID Handbook, second edition, John Wiley and sons Ltd., West Sussex England 2003.

38. *Nagy P., Berstein W., Caban J., Klein R., Mezreich R. & Park A.*, Radio Frequency Identification Systems Technology in the Surgical Setting, SurgInnov 2006, 13:61, at p. 66, available at http://sri.sagepub.com/content/13/1/61. The authors add, however, that research should be done so that implantable tags have a mechanism to render them inoperable. Id.

39. US Food and Drug Administration. Medical devices: general hospital and personal use devices: classification, Federal Register, 2004; 69(237): 71702-4.

40. Report, id. See note 32.

41. There are numerous examples where people have waived complete anonymity in return for some perceived benefit, see *Hardy M.*, Wireless struggles with security, March 2005, cited in *Nagy et al.*, id., p. 67.

hospital staff especially when they are in need of immediate treatment[42]. The question of securing informed consent to the implant of an RFID chip remains open, of course, when the patient is mentally impaired-in this case, the standard rules on incompetence apply-of course, with all their endless difficulties in application. But even leaving the incompetence question aside, we have evidence from research on people who have consented to be implanted that "...some patients are chipped with adequate knowledge how the system works....patients have considerable misunderstanding about the technological capabilities of the implants for their health and safety..."[43].

It is interesting to note that there is evidence that the RFID implant could be connected to health hazards. Firstly, there is evidence that emitting radio waves could cause tumors and therefore, patients should know of potential risks before being implanted[44]. Laboratory research in mice and rats injected with microchips concluded that these animals at times developed cancerous tumors around the microchips[45]. Perhaps the only safe statement is that we need a twenty years study of the effects of microchips in humans in order to offer some safe evidence of this link in the case o humans[46]. In parallel, there is evidence that the RFID systems may interfere with the proper function of other medical devices in a hospital e.tc. Especially in the ISU unit, there is evidence that RFID technology is capable of inducing potentially hazardous incidents in medical devices[47]. All these are matters which remain open to new research but at least, patients should be aware of this kind of dangers before consenting to be implanted.

---

42. *Monahan T. & Wall T.*, Somatic Surveillance: Corporeal Control through Information Networks, Surveillance and Society, Part 1, 4(3): 154-173, p. 165, available at http://www.surveillance-and-society.org. Accessed on June 10, 2013.

43. *Monahan & Fisher*, id., 374. See note 33. This is also an important quotation from the article: "...as with many other informed consent procedures the special setting of a professional healthcare context conveys to patients messages of medical authority that encourage them to trust medical professionals and downplay risks indicated in informed consent forms...", p. 165.

44. *Foster KR & Jaeger J.,* Ethical Implications of implantable radiofrequency identification in humans, Am. J. Bioeth. 2008; 8: 44-48.

45. *Lewan T.*, Chip Implants Linked to Animal Tumors, The Washington Post, http://www.hwshingtonpost.com/wp-dyn/content/article/2007/09/08/AR2007090800997_pf.html. Accessed June 10, 2013.

46. *Lewan*, id. See note 45.

47. *Remko van der Togt, Erki van der Lieshout, Renouk Hensbroek, E. Beinat, J.M. Binnekade & P.M.J. Bakker,* Electromagnetic Interference From Radio Frequency Identification Inducing Potentially Hazardous Incidents in Critical Care Medical Equipment, JAMA. 2008;299(24): 2884-2890.

When it comes to tagging hospital personnel, research has indicated that the staff has shown unexpected resistance to the installation of RFID tags on both medical equipment and personnel, resistance that could be understood in terms of work intensification that seemed to accompany its implementation and the creation of a "Big Brother" atmosphere in hospitals[48]. What promoters of the systems call "workflow management" in this case cannot escape the true characterization of surveillance and control, at least as a result, and there is no doubt that, no matter the possible benefits, hospital personnel has understood the RFID systems on persons as such[49]. Interestingly, these systems apply almost exclusively to patients and nurses and almost never to physicians or hospital management[50].

3. Societal implications and facets of medicine

Although as stated, the main lens the RFID chips have been analyzed from the scholarly community is privacy, the truth is the matter raises some other and perhaps more important questions of a different nature. One initial thought is that we need to be very careful in mingling people and objects together when it comes to RFID tagging. Reading the relevant literature one should sometimes stop and think whether it is legitimate to speak of tagging people in the same way we tag boxes of cereal. And I stress this point because very often in the texts, even in the healthcare context, where patients are so much more vulnerable, we do see the subject analyzed without a clear distinction of whether we deal with people (patients/personnel) or medical equipment. For example, we read:

> "*…To make healthcare management systems functional and successfully operational, RFID solutions can be used to reduce operating costs through management of patients, employees, equipment, medications, and records to improve*

48. *Fisher*, id. At p. 83. See note 25.

49. "…Nurses in particular express concern that they are overly scrutinized by these tracking technologies. They also indicate that the systems are based upon rational management models that do not accurately match the messy realities of hospitals. In addition to being watched by administrators, some nurses experience an intensification of labor because the task of keeping RFID operational often falls upon their already overburdened schedules…. In cases where the staff are being tracked by the RFID systems, nurses describe feeling like "big brother" is watching them as they spend time with patients, take unofficial rest breaks between patients and take official breaks during their shifts. Several hospitals with strong nurses' unions have even blocked the implementation of RFID systems because of current evidence that the burden of these systems falls disproportionately on nurses…", *Fisher & Monahan*, Tracking the social dimensions of RFID systems in hospitals, International Journal of Medical Informatics 77 (2008), 176-183, at 180.

50. *Monahan T.*, Dreams of Control at a Distance: Gender, Surveillance and Social Control, Cultural Studies, Critical Methodologies, volume 9, n. 2 April 2009, 286-305, at 294.

tracking and tracing, and preventing the lost of resources under any circumstances….[51]*".*

This way of dealing with the matter is rather common in the literature-jumbling patients and personnel along with medical equipment. It reflects an inability of the acute need to clarify the differences between the two classes, of people and objects.

So when it comes to patients, the risk of not "listening" to what the patient has to say but to seek information only in the patient's electronic health record, to which the RFID chip leads has also been documented. Generally, the use of these chips seems to reinforce the distancing between the healthcare worker and the patient. The need to look at a patient's face and listen to her voice in a way disappears, when everything the healthcare worker needs is the data contained in the database, where the RFID points at. When you use a chip like this to measure whether the patient is walking well enough as recovering after surgery, the next step is not to use your own senses as a physician and nurse at all: again, not to look, not to touch, not to feel, not to listen to what a patient says. Note the enthusiastic declaration of yet another possible use of a RFID chip:

"…As the patient recovers, he or she is frequently encouraged to exercise and walk around the hospital during recovery. As a patient moves about, his or her movements can be tracked by RFID readers scattered throughout the facility. Such information can be logged and can give the tending physicians an idea of how much physical activity the patient has engaged in…[52]*".*

So the 'technological imperative' of RFID implants comes almost naturally, as the patient doesn't even have *a name* you know-you need a RFID chip to ascertain you are operating upon the right person, as you need an RFID chip to know where a patient *is* in the hospital or hospital surroundings. This may be a little step from the idea of using RFID chips to monitor people infected by HIV so that the chances they infect are people be reduced, as proposed in 2008 by the legislature in Indonesia[53].

51. *Yahia Zare Mehrjerdi,* Radio frequency identification: the big role player in health care management", Journal of Health Organization and Management, 2011, vol. 25 iss. 5, pp.490 – 505, Italics mine.

52. *Cangiolosi et at.*, Applying…., see note 28, p. 1053.

53. This would not be possible as yet, anyway, as there is no RFID chip today that could operate as a GPS. See generally *Tedjasukmana J.,* Papua Proposal: a Microchip to Track the HIV positive, Time, http://www.time.con/time.world/article/0,8599,1862347,00.html. Last access June 10, 2013. The proposal was rejected the Government, People, 2008, 12.8.

And yet, how many are the medical errors happening because the physicians *do not listen* to information offered by the patients, and do not physically touch and examine them, but instead they rely exclusively to information coming from diagnostic exams and medical histories in databases? The case that RFID technology will possibly diminish even more trust from physicians to patients has already been documented, as healthcare providers have indicated that they would be more likely to trust the information contained in the system than information gleaned from patients themselves[54]. All this comes at a time when, as noted, little research exists on the efficacy of RFID implants for improving patient care, the organizational arrangements necessary to support their use or the ethical issues that may arise for their use[55].

While much publicity has been given to these high-profile cases of operating upon the wrong patient e.tc., these errors are in fact relatively rare. A seminal study[56] estimated that such errors occur in approximately 1 of 112,000 surgical procedures, infrequent enough that an individual hospital would only experience one such error every 5-10 years. This should be taken into account when discussing benefits and costs of RFID technology in healthcare. Perhaps resources should be better dedicated to enhance trust and discussion between physicians and patients, as this would almost surely reduce medical informed consent claims, which are mostly based on breaches of trust between a doctor and a patient and misinformation given by doctors to patients.

Finally, it is important to stress that whereas the RFID implantable chip may be used in healthcare, but it should never be confused with a medical device. As aptly said, "…it is something which is an identifier that can be applied in a way that has a good medical outcome but it is not like a scalpel…"[57]. No, an RFID chip is not a scalpel[58], although every scalpel, for better or for worse, may well be carrying a RFID tag in the perhaps not so distant wonderful technological future.

---

54. *Monahan & Fisher*. id. , 373, 375. Note 33.

55. *Monhan T. & Wall*, id., 165. Note 42.

56. *Kwaan MR, Studdert DM, Zinner MJ, Gawande AA*, Incidence, patterns and prevention of wrong-site surgery, Arch. Surg. 2006l 141;353-358.

57. As stated by Dr. Ian Kerr, the Canada Research Chair in Ethics, Law and Technology, see Health-care chips could get under your skin, 2006, Medicine and Health, available at www.physorg.com/news69341086.html. Last access June 10, 2013.

58. And it is not "just another technology that provides practical value for me like my BlackBerry", as Halamka John, MD, an emergency room doctor at Beth Israel Deaconess stated, commenting on the RFID implant he had in the back of his right arm, see *DeNoon D.*, Chip Implants: Better Care or Privacy Scare? available at http://www.foxnews.com, last access June 10, 2013.