RFID and Privacy:
Guidance for Health-Care Providers

January 2008

RFID and Privacy: Guidance for Health-Care Providers

Foreword

Health-care providers around the world are recognizing the benefits of adopting Radio Frequency Identification (RFID) technology into their operations, in order to enhance health care service delivery. The availability and use of innovative new RFID-enabled information technology applications are helping providers to track medical equipment and supplies more efficiently, verify the authenticity and administration of drugs, and improve patient safety and security, such as by using RFID-enabled identification bracelets for newborns and patients. However, as the benefits of RFID uses and applications are realized, concerns are also being raised about the potential privacy implications associated with use of this technology, especially when RFID tags are linked to identifiable people.

In the autumn of 2006, I was approached by Victor Garcia, Chief Technology Officer for Hewlett-Packard (HP) Canada, seeking the expertise of my office in how potential privacy issues could be identified and safeguards developed and implemented into the usage of RFID technology. I was more than willing to contribute my insight and expertise because, as Commissioner, part of my mandate includes reaching out to external organizations. I have also found it beneficial to assist both public and private organizations working on emerging technologies, and to always be proactive whenever possible – to develop effective guidelines and codes of conduct before any problems arise. Further, I was also interested in working with HP given that it is an organization that takes the protection of privacy very seriously, having a history of working alongside legislative and standards bodies, partners, customers, and NGOs to help drive the adoption of privacy principles to protect consumer privacy rights. Specifically regarding HP's work with RFID, I was encouraged by its corporate values in that individuals should always be given notice about the presence of RFID tags, and where possible, have the choice to remove or deactivate RFID tags. HP products with an RFID tag on the box are always accompanied by an EPCglobal logo, which alerts the consumer to the presence of the tag. Lastly, I was also impressed by the fact that my colleagues at HP and I share the same belief – that being visible about RFID use will breed confidence in the technology, while being secretive will heighten the misconceptions and fears.

My work with RFID began in 2003 when I released *Tag, You're It: Privacy Implications of Radio Frequency Identification (RFID) Technology*, and I first identified the potential privacy concerns raised by RFID technology. Since then, I have gone on to work with a number of organizations such as EPCglobal Canada, with whom I consulted when I wrote *Privacy Guidelines for RFID Information Systems*

(RFID Guidelines). My office has also helped to shape policy and ideas, from RFID tags in Ontario's public libraries to lectures on how to implement privacy protections in RFID systems. This publication is a continuation of my ongoing work with RFID. For many months, IPC and HP staff worked hard to examine questions regarding RFID privacy protections. The result is this co-authored document.

The essential purpose of this publication is to assist the health-care sector in understanding the current and potential applications of RFID technology, its potential benefits, its privacy implications, and steps that can be taken to mitigate potential threats to privacy. I, and my co-author, Victor Garcia at Hewlett-Packard, sincerely believe that this document will serve as a benchmark for considerations relevant to the application of, and the privacy issues associated with, RFID technology in health care.

During the time I was working toward making the *Personal Health Information Protection Act (PHIPA)* a reality, I repeatedly stated that, "I believe in the necessity of *PHIPA* not only because I am the Commissioner, but also because I am a patient." I believe that the same sentiment also applies to this document. While I, as a patient, would welcome the prospect of RFID technology improving my health-care services, I, as Commissioner, also believe that we must ensure the deployment of this technology does not infringe upon our privacy.

Ann Cavoukian, Ph.D.
Information and Privacy Commissioner of Ontario

About the Authors

Information and Privacy Commissioner of Ontario (IPC)

In her mandate and role in relation to personal health information, the Information and Privacy Commissioner of Ontario has the authority to oversee compliance with the *Personal Health Information Protection Act (PHIPA)*. The *Act* authorizes the IPC to review complaints about a person who has contravened or is about to contravene *PHIPA*, and review complaints related to the right of individual access and correction. It also authorizes the IPC to engage in or to commission research into matters affecting *PHIPA*, conduct public education programs, and provide information on *PHIPA* and its role thereunder.

Hewlett-Packard (HP)

One of the world's largest IT companies, Hewlett-Packard (HP) is not only involved in the development of innovative RFID technologies and applications, it is also committed to improving health care by focusing on: delivering solutions that allow health-care providers better access to patient information by integrating systems, data, processes and people; providing staff and patients with secure access to information, data and applications; and transforming business processes and IT to better serve the public interest.

Introduction

Information and communications technologies (ICTs) are transforming the world we live in through revolutionary developments in bandwidth, storage, processing, mobility, wireless, and networking technologies.

The health-care sector has recognized the value of new technology in the delivery of health care. For example, globally, billions of dollars are now spent annually on advanced diagnostic and treatment equipment. Until recently, however, ICTs were limited to administrative and financial applications and played only a small role in direct care for patients. But we are beginning to see an evolutionary – perhaps even revolutionary – change in how health care is delivered.

Health-care providers around the world are undergoing a digital transformation, harnessing cutting-edge IT to increase operational efficiencies and save lives. For example, they are replacing expensive, hard-to-share and easily lost X-ray films with digital images that can be effortlessly and securely shared, stored, transmitted and accessed. They are also moving away from an environment dominated by hand-written notes and physician orders to one where staff use ICTs to document patient records and enter and process orders. Thanks to ICTs, the vision of comprehensive and instantly available electronic health records is now within reach.

But the digital transformation is about much more than just software applications. It involves taking advantage of advanced technology such as RFID to imaginatively meet a host of needs. Invented over 60 years ago, RFID is fundamentally a technology for automatic identification that can be deployed in a nearly unlimited number of ways. The technology is starting to hit its stride, finding a wealth of new uses and applications related to automated identification, safety and business process improvement.

Patient safety is one of the most critical issues in the health-care sector today. There is a mounting concern about medical errors, such as from the administration of incorrect medications or dosages, or from patients being misidentified. A 1999 study of 1,116 hospitals by the United States Institute of Medicine suggests that more than 44,000 deaths occur each year in the United States as a result of in-hospital medication errors.[1] Canadian estimates put the figure at 700 deaths per year due to medication errors.[2] A 2002 study of medication errors at 14 acute-care hospitals in Ontario counted over 4,000 errors, only 800 of which were

1 Institute of Medicine, *To Err Is Human: Building a Safer Health System*, Washington, D.C.: National Academy Press, 1999.

2 David U, BSc Phm, MSc Phm., (President and CEO, Institute for Safe Medication Practices Canada), *Medication Error and Patient Safety*, Longwoods Publishing, Vol. 2, No. 1, at: **www.longwoods.com/product.php?productid=16442**

counted as adverse drug effects.[3] A similar study conducted at the Children's Hospital of Eastern Ontario, published in 2003, counted over 800 medication errors during a six-year period.[4] RFID technologies may offer remedies for these patient safety problems.

Operational inefficiencies, in some cases due to the inability to rapidly find and track medical equipment, are also a concern for the health-care sector. It has been estimated that the theft of equipment and supplies costs hospitals $4,000 per bed each year and with over 975,000 staffed beds in the U.S., this represents a potential loss of $3.9 billion annually.[5] Considerable time and effort is spent searching for valuable mobile medical assets, and in maintaining an accurate and up-to-date inventory – human resources that might otherwise be better dedicated to more productive ends. Once again, RFID technologies can help provide cost-effective solutions.

Increasingly, there is considerable interest in exploring the uses of new technology to better understand processes, achieve greater operational efficiencies and improve patient safety.

In the health-care sector, RFID technology is already being used to rapidly locate medical equipment and devices, track surgical equipment, specimens and laboratory results, identify and verify the authenticity of pharmaceuticals (including for stock rotation and recalls), and to ensure that the right medicine, in the right dosage, is given to the right person at the right time. Other applications include positively identifying patients, prescribing and checking drug interactions at the point of care, quickly checking a patient's blood type, matching newborn infants with their parents, and triggering a lock-down after the unauthorized removal of an infant from a secured area. Finally, RFID technology is being effectively used to help improve patient registration and management processes at hospitals, leading to analysis of bottlenecks, improvement in flow and reduction in wait times.

3 Joan A. Marshman, David K U, Robert W.K. Lam, and Sylvia Hyland, *Medication Error Events in Ontario Acute Care Hospitals*, Can J Hosp Pharm 2006;59:243-50, at:
www.ismp-canada.org/download/Medication_Error_Events_in_Ontario_Acute_Care_Hospitals.pdf

4 W. James King, MSc, MD*, Naomi Paice, MD*, Jagadish Rangrej, MMath, Gregory J. Forestell, MHA | | and Ron Swartz, BScPharm, *The Effect of Computerized Physician Order Entry on Medication Errors and Adverse Drug Events in Pediatric Inpatients*, in PEDIATRICS Vol. 112 No. 3 Sept 2003, pp. 506-509, at:
http://pediatrics.aappublications.org/cgi/content/abstract/112/3/506

See also: Health Canada, Look-alike Sound-alike Health Product Names, at:
www.hc-sc.gc.ca/dhp-mps/alt_formats/hpfb-dgpsa/pdf/brgtherap/lasa-pspcs_factsheet-faitsaillant_e.pdf, and Institute for Safe Medication Practices Canada (ISMP Canada), Canada Safety Bulletin, Vol. 6, Issue 4 (July 2006), *Eliminate Use of Dangerous Abbreviations, Symbols, and Dose Designations*, at:
www.ismp-canada.org/download/ISMPCSB2006-04Abbr.pdf

5 *RFID: Coming to a Hospital near You*, Sun Microsystems press, April 2004.

Pilot projects are underway in Canada. In January 2006, Hamilton Health Sciences, in conjunction with the RFID Applications Lab at McMaster University, launched a multi-phased multi-year RFID initiative to explore and assist in development of better business intelligence tools for health care. The initial effort was focused on exploring the economic and technical feasibility of using RFID to track valuable mobile assets in real-time. Expected efficiency benefits include labour savings, reduced capital expenditure for equipment, equipment and item loss prevention, and process improvements. Future phases of the project are aimed at looking at optimizing and improving processes related to daily operations such as asset management as well as patient care by using evolving technology as an enabler. These may include using RFID for patient identification and pandemic planning, depending on the results of their planned privacy study.

In January 2008, London (Ontario) Health Sciences commenced the first implementation phase of their RFID strategy, with an RFID pilot deployed by Hewlett-Packard designed to track infusion pumps and other critical medical equipment in real-time, providing business intelligence and operational data based on the location and utilization of equipment. London Health Sciences' vision for the application of RFID within their facilities includes leveraging automatic identification and tracking systems to achieve better use of medical equipment, equipment and item loss prevention, and process improvements, eventually leading to increased patient safety in proper balance with privacy protection, confidentiality and data security.

Perhaps the most intensive use of RFID technology would be in a contagion research facility, where all people and items – and the interactions among them – can be closely tracked and monitored (some pandemic emergency scenarios also call for fine-grained location, tracking and audit capabilities). Perhaps the most innovative RFID technologies being developed today are biosensors – specialized RFID chips implanted into bodies to monitor and transmit critical health conditions.

These publicized applications of RFID technology in Canada and around the world have highlighted the potential for widespread use of this technology in the health-care sector. Factors prompting the publication of this document include:

- The increasing availability of RFID-based solutions for the health-care sector;
- The growing interest in the use of this technology by health-care providers; and
- The concerns that have been raised about the potential privacy implications associated with the use of RFID technology in the health-care sector.

This paper provides a balanced analysis of RFID technology by examining a wide variety of RFID applications in the health-care sector from around the world, and organizing them into three broad categories:

- RFID technology to track things;
- RFID technology to track things linked to people; and
- RFID technology to track people.

The paper also identifies the benefits and potential privacy issues associated with this technology and the steps that may be taken to mitigate the threat to privacy.

What Is Privacy?

Informational privacy defined

Informational privacy is the right of an individual to exercise control over the collection, use, disclosure and retention of his or her personal information, including his or her personal health information. Personal information (also known as personally identifiable information or "PII") is any information, recorded or otherwise, relating to an identifiable individual. Almost any information, if linked to an identifiable individual, can become personal in nature, be it biographical, biological, genealogical, historical, transactional, locational, relational, computational, vocational, or reputational. The definition of personal information is quite broad in scope. The challenges for privacy and data protection are equally broad.

How privacy is regulated in the health-care sector in Ontario

On November 1, 2004, the *Personal Health Information Protection Act (PHIPA)*[6] came into effect in the province of Ontario. *PHIPA* provides individuals with control over the collection, use and disclosure of their personal health information by requiring persons and organizations in the health sector, defined as health information custodians, to collect, use and disclose personal health information only with the consent of the individual to whom the information relates, subject to limited exceptions. It also provides individuals with the right to access and require correction of their personal health records, subject to specific exceptions.

PHIPA defines "personal health information" as identifying information about an individual that, among other things, relates to the physical or mental health of the individual, relates to the provision of health care to the individual, identifies a provider of health care to the individual, identifies the substitute decision-maker of the individual, or is the individual's health number.

It defines a "health information custodian" as a person or organization listed in *PHIPA* that has custody or control of personal health information. Examples of health information custodians include health-care practitioners, hospitals, psychiatric facilities, long-term care homes, pharmacies, laboratories, and ambulance services.

6 *PHIPA* text available at: **www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_04p03_e.htm** and *A Guide to the Personal Health Information Protection Act* available at: **www.ipc.on.ca/images/Resources/hguide-e.pdf**

PHIPA reflects worldwide privacy criteria, such as the principles of fair information practices set forth in the *Canadian Standards Association Model Code for the Protection of Personal Information*[7] and the *Global Privacy Standard*, an effort of the international privacy and data protection commissioners, led by the IPC, to harmonize the various privacy codes and practices currently in use around the world.[8]

Obligations of the health-care sector in relation to personal health information

Health information custodians are required, under *PHIPA*, to collect, use and disclose personal health information only with the consent of the individual to whom the personal health information relates, subject to limited exceptions. They are also required to comply with the wishes of an individual who withholds or withdraws consent, or who gives express instructions that the information must not be used or disclosed for health-care purposes in certain circumstances.

PHIPA also prohibits health information custodians from collecting, using or disclosing personal health information if other information will serve the purpose and requires that only the information that is reasonably necessary be collected, used, or disclosed. Custodians are required to take reasonable steps to ensure that personal health information is protected against theft, loss and unauthorized use or disclosure, ensure that records are protected against unauthorized copying, modification and disposal, and retain, transfer, and dispose of health information in a secure manner.

In addition, *PHIPA* requires health information custodians to provide individuals with the right to access their records and have them corrected subject to specific exceptions.

Obligations of electronic services providers in relation to personal health information

Suppliers of electronic services (who are not agents) that enable the health information custodian to collect, use, modify, disclose, retain or dispose of personal health information are bound by certain obligations in *PHIPA*. These include not using personal health information except as necessary in the course of providing services, not disclosing personal health information, and not permitting employees or others acting on the supplier's behalf to have access to personal health information unless they agree to be bound by these restrictions.

Further, if the supplier is a "health information network provider," providing services to two or more health information custodians primarily to enable them to disclose personal health information to one another electronically, regardless of whether or not it is an agent, the "health information network provider" is subject to further obligations prescribed in regulation.

7 Available at: **www.csa.ca/standards/privacy/code/**
8 Available at: **www.ipc.on.ca/images/Resources/up-gps.pdf**

What Is Radio Frequency Identification (RFID)?

RFID technology fundamentals

RFID is a contactless technology that uses radio frequency signals to transmit and receive data wirelessly, from a distance, from RFID tags or transponders to RFID readers. RFID technology is generally used for automatic identification and to trigger processes that result in data collection or automation of manual processes.

Key advantages of RFID-based systems for health-care delivery include:

- Accurate identification without the need to touch (or even see) the RFID tag;
- Sensors can be incorporated into RFID tags to record temperature or identify positioning;
- Data stored inside RFID tags can be encrypted, modified and rewritten on demand;
- Tags are recyclable and can be made difficult to counterfeit;
- Special devices are required to read RFID tags, increasing privacy in some cases (e.g., in comparison to human-readable information).

The most common application types, grouped according to the purpose of identification, are presented below:

Purpose of Identification	Application Type
Determine the presence of, and identify, an item	Asset management, safety
Determine the location of an item	Tracking, emergency response
Determine the source of an item	Authenticity verification
Ensure affiliated items are not separated	Matching
Correlate information with the item for decision-making	Process control, patient safety
Authenticate a person holding a tagged item	Access control, ID verification

Many RFID applications will often span multiple purposes.

An RFID system is typically composed of:

1 RFID tags, which can be Passive, Active or Semi-Active, typically containing a unique identifying data string and potentially additional data;

2 RFID readers and writers, which can be wireless, handheld or fixed reader/antenna devices;

3 An infrastructure, including middleware, that permits RFID readers and writers to process data to and from the RFID tags, manage communications, access control and security, connect to back-office applications, and take actions on the basis of that data.

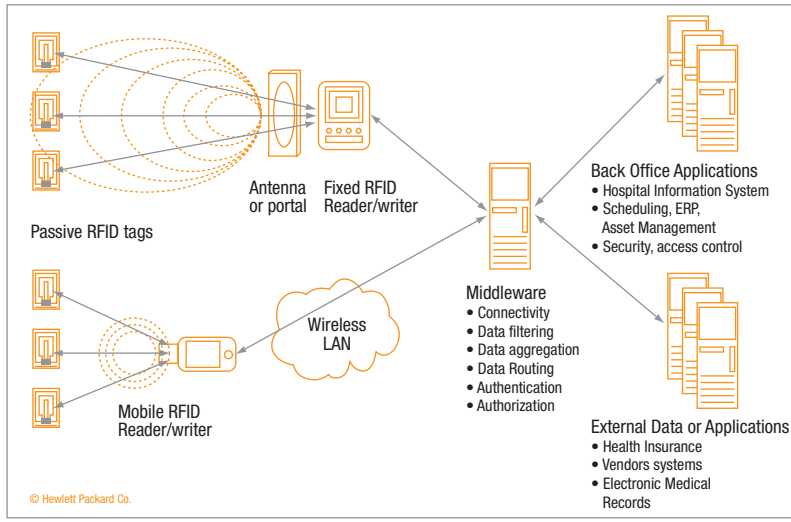


Figure 1 – Typical Passive RFID system

It is important to note that the RFID tag and reader are only the up-front, visible part of an RFID system, which often connects through a wired or wireless network to a back-office application and one or more databases or hospital information systems.

There are some important types and varieties of RFID tags and associated RFID information technologies and systems. These are outlined briefly below.

1. Passive vs. Active RFID tags

RFID tags can be Passive (non-battery powered), Active (battery-powered), or Battery-Assisted Passive (dual mode). Passive tags, which are by far the most common, are the simplest and least expensive to manufacture and use. They contain a chip and antenna on a substrate, typically attached to a label or bracelet, are typically classified within Low-Frequency, High-Frequency or Ultra-High Frequency groupings, and comply with standards such as ISO or Electronic Product Code (EPC). To transmit their data payload, passive tags use radio energy supplied by RFID interrogators or readers. Passive tags typically contain small data payloads, can be read-only or read-write, and must be physically close to the reader to communicate effectively (Hi-Frequency tag read-ranges can vary from 3 to 30 inches, Ultra-High-Frequency tags can be read up to 15 to 20 feet from the reader-antenna). The new generation of Battery-Assisted Passive tags can contain larger amounts of data, and transmit over longer distances.

Active RFID tags, or transponders, contain a battery and can be configured to transmit their information at given time intervals or react to an awakening signal or event. The tag's battery life typically ranges from one year to over five years, depending on the frequency that they transmit data. These tags are much more expensive than passive tags, but provide additional functionality. The tags can be read at longer

distances (e.g., 100 to 500 feet), can hold larger amounts of data and can contain integrated sensors (e.g., temperature, motion, tamper-detection, etc.). Some active tags can provide two-way communications using customizable buttons, LED lights, or buzzers integrated into the tag, similar to a pager. This technology is typically used in high-value asset management solutions or real-time medical equipment tracking solutions, including detection of presence, zone coverage or real-time location services (RTLS). RTLS systems function in a manner similar to GPS location systems, measuring the signal strength from the tag received by three or more readers and graphically displaying the current or historical location of the tag on a map. Some RTLS systems use proprietary antennas and readers and others can leverage an existing Wi-Fi infrastructure to communicate with the tags. The systems can be configured to provide customized monitoring and alerting of events, such as battery power status, a tag entering a restricted area, a tag falling to the floor, or a tag being removed from an object without authorization.

All of the described types of tags have important implications for privacy and security.

2. Referential vs. non-referential RFID systems

The term "referential" is used for RFID systems using tags that typically contain a unique "key" or semi-random data string, which allows retrieval of relevant information from an application or database. Referential RFID systems are the dominant type in use today. As suggested by Figure 1 above, the data on the tags serves as a pointer or "reference" to a centralized storage and processing systems located elsewhere on the network. The information stored on the tag allows retrieval of information from the database, file, or document contained in the back-office system, or logic embedded inside a local or remote information system or process. For example, an RFID-enabled proximity card can contain a serial number that, when waved near an antenna connected to a reader, triggers that reader to collect the data and send it to a computer or server where the data is compared against stored values. If there is a positive match, an action is then performed, such as unlocking the door to an office or opening a patient's medical record. If the network is down, the system may not function as desired, as the information contained in the tag may not be sufficient to trigger the desired action.

By contrast, "non-referential" RFID systems are able to store all or some of the data needed for systems operation in the tag's memory, and may contain logic running on mobile devices or the tag itself. This functionality allows decisions to be made based on the information stored in the tag, without any need for linked networks and back-end databases to function, which can prove useful if the network is down, or the data can not be accessed online. Non-referential systems contain functionality to synchronize the information between the tag and a back-office database or application and encryption is typically used to protect against unauthorized access to the data.

Both types of RFID systems have implications for personal information and privacy.

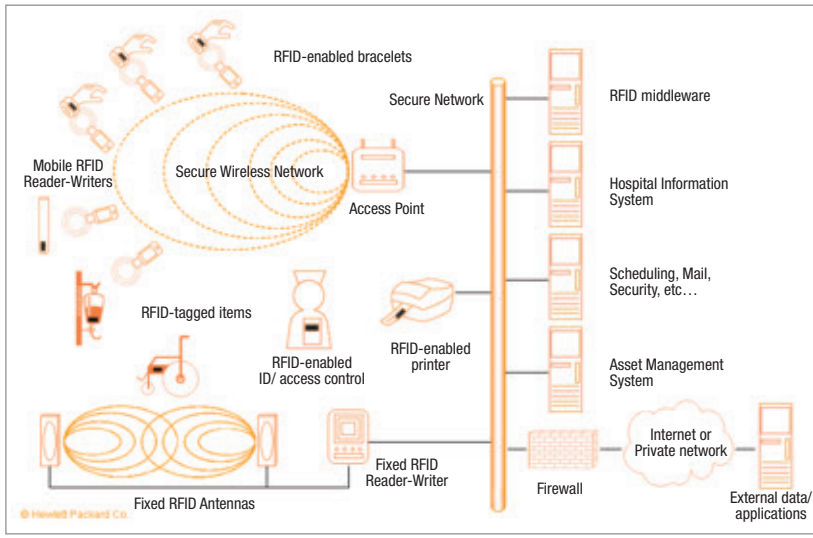
3. Closed vs. Open Loop applications

A closed-loop RFID application – the most common type – is any RFID system that is deployed entirely within a single organization, rather than across several organizations. Closed-loop RFID information systems may involve the use of either standards-based or proprietary tags, encoding formats, transmission protocols, and processing middleware.

An open-loop RFID application, by contrast, is intended to function across organizational boundaries, requiring adoption of common standards and information-sharing protocols. RFID deployments for supply-chain management, in which an item is tracked across various organizations in a range of locations, are a classic example of open-loop RFID application.

Just as the authenticity of the RFID-enabled proximity card is verified against a back-end database, the authenticity of a pharmaceutical product may be verified to ensure that the product is not counterfeit. A record of access can be kept for billing purposes or to record the time that someone entered a particular building or room. The travels of an RFID-tagged item can be monitored and tracked across time and distance through periodic reads of the tag and correlation of its unique identification in a database. This is what occurs when RFID-tagged supplies and inventory are shipped from a production facility to a distributor to a retailer, providing visibility and accountability throughout the entire supply chain.

Sample RFID System



RFID Technology vs. Bar Codes

Bar code systems are commonly used in health-care settings, but are known to have technical limitations such as inaccessibility when a patient covers the wrist band with his or her body or the bar code is curved around a wrist band. In such

cases, manual entry of the patient ID is required, or the patient must be awaken or touched to facilitate reading of the bar code, potentially increasing the risk of nosocomial infections. Bar codes also have limited storage space for information and can wear out after protracted use. They do not facilitate modification and updating of information (unless the bar code is reprinted). These limitations consume resources that could otherwise be spent on other tasks, increase the risk of human error, and increase operating costs.

Generally speaking, RFID represents a next-generation improvement over traditional bar codes. Some differences between the two technologies are identified below.

Bar Coding	RFID
• Requires line of sight	• Line of sight not required
• Scan one item at a time	• Multiple items at a time
• Inexpensive	• More expensive
• Widely used	• Emerging application in health care
• Standards-based	• Standards developing
• Read only	• Digital, read-write capable
• Depends on external data store	• Can store data or trigger access to external data
• Provides licence plate information only	• Can store relevant data (serial #, loc., status, etc.)

RFID and Privacy

RFID implementation considerations

There are five general implementation issues associated with deploying RFID technology:

1 **Cost** – The cost of the technology (tags, readers, middleware, consulting, operational process design, troubleshooting, training, etc.) will impact return on investment (ROI) and value.

2 **Integration with hospital information or other back-office systems** – Legacy information systems may need to be modified or re-engineered to accommodate the RFID system, technology, and information.

3 **Reliability** – Depending on the operating environment, the intended purposes, the technology contemplated, and the deployment method being considered, RFID technologies may not deliver sufficient accuracy or performance results to be suitable for mission-critical applications and uses.

4 **Security** – RFID tags are susceptible to many of the same data security concerns associated with any wireless device[9]. Passive tags in particular are considered to be "promiscuous" – automatically yielding their data to any device that queries the tag, raising concerns about skimming, interception, interference, hacking, cloning, and fraud, with potentially profound implications for privacy. While a variety of security defences exist, such as shielding, tag encryption, reader authentication, role-based access control, and the addition of passwords, these solutions can raise complexity and costs.

5 **Privacy** – If RFID tags contain personal information, which could include health information, or data linked to personally identifiable individuals, without the proper security or integrity mechanisms in place, privacy interests become engaged. Personal health information is among the most sensitive types of information. As such, it requires stronger justifications for its collection, use and disclosure, rigorous protections against theft, loss and unauthorized use and disclosure, strong security around retention, transfer, and disposal, and stronger, more accountable governance mechanisms.

Privacy-relevant properties of RFID systems

There are certain fundamental properties of all RFID information systems that are particularly relevant to privacy, regardless of the specific technology, application type, or deployment scenario.

1 Health-care providers must realize that RFID systems are a key part of an overall information system. Consequently, a holistic systems approach to privacy is warranted, rather than a strict focus on the interaction between tag and reader.

2 RFID tags contain unique identifiers, indicating not only the presence of an object, like an anti-theft tag, or a class of objects, like a product bar code, but also an individualized serial number. The ability to uniquely identify individual items has privacy implications when those items can through inference automatically be associated with people.

3 RFID tag data can be read (and sometimes written) at a distance, without "line-of-sight" and through many camouflaging materials, potentially without the knowledge or consent of the individual who may be carrying the tag. This has potent implications for informed consent.

4 RFID information systems can also capture time and location data, upon which item histories and profiles can be constructed, making accountability for data use critical. When such systems are applied to people, it may be viewed as surveillance (or worse, depending on what is done with the data).

9 For a discussion about various forms of wireless technologies and the privacy and security considerations in their use, see *IPC Fact Sheet #14 – Wireless Communication Technologies: Safeguarding Privacy & Security* (August 2007), available at: **www.ipc.on.ca/images/Resources/up-1fact_14_e.pdf**

To first understand privacy and security risks, and then to mitigate these risks, we must always follow the (personal) data as it flows throughout the entire information system: what data is collected, how and for what purposes, where it is stored, how it is used, with whom it is shared or potentially disclosed, under what conditions, and so forth. This is referred to as the information life-cycle, and the disposition and governance of personal health information throughout its life-cycle lies at the heart of most information privacy concerns in the health care environment.

RFID systems are, fundamentally, information systems put in place by organizations to automatically capture, transmit and process identifiable information. Informational privacy involves the right of individuals to exercise control over the collection, use, retention and disclosure of *personally* identifiable information by others. There are inherent tensions between the, at times, competing interests of organizations and individuals over the disposition of the information, especially over the undisclosed or unauthorized revelation of facts about individuals and the negative effects they may experience as a consequence.

As was described in a recent European study on the many uses of RFID technology, RFID information technologies can exacerbate a power imbalance between the individual and the collecting organization.[10]

General approach and framework to building privacy in early

Building privacy into information systems and technologies, whether RFID-enabled or not, begins at the top of the organizational decision ladder, and at the early stages of project design and implementation. A comprehensive, multidisciplinary approach is required. The steps outlined here provide a high-level approach and general framework for building privacy into information technologies and systems.

As a framework, it is useful for general orientation and planning purposes, and may be used as a starting point for deeper analyses, according to the specific objectives, operational characteristics, and other parameters of the RFID proposal or project in question.

1 Clearly define, document and limit purposes for collecting and using personal data, in order to minimize the potential for privacy invasion. The purposes identified should meet the tests of necessity, effectiveness, proportionality, and no less-invasive alternative.

2 Develop a comprehensive and realistic project management plan, with the pivotal involvement of a knowledgeable privacy officer, with sufficient authority and resources.

10 See *RFID and Identity Management in Everyday Life: Striking the balance between convenience, choice and control,* study by the (July 2007) European Parliament Scientific Technology Options Assessment (STOA), IPOL/A/STOA/2006-22.

3 Identify all information security and privacy risks throughout the data life-cycle, including risks from inside the organization as well as external sources.

4 Conduct a comprehensive Privacy Impact Assessment (PIA) of the entire system at the conceptual, logical and physical stages of its development, with a clear plan and timetable for addressing identified risks.

5 Build privacy and security in at the outset. This means incorporating the principles of fair information practices into the design and operation of an RFID information system, and the policies that govern its operation.[11]

6 Implement appropriate operational and systematic controls that can be measured and verified, ideally by independent entities, if necessary.

7 Review the operation and effectiveness of the RFID system, as well as related networking, data storage, wireless transmission, and data backup systems on a regular basis.

RFID systems may need to be highly customized to support the business processes they automate, and will depend on the types of back-office systems, medical information system, scheduling or similar support systems they must interface with. In many cases, a "one-size-fits-all" approach will not work across all health-care implementations. Good privacy and security practices, integrated with strong project management skills, can help health-care providers manage RFID risks to an acceptable level.

The section that follows goes into more detail on the privacy considerations specific to the RFID health-care application.

RFID Applications in the Health Sector

Health-care providers around the world have been using or testing RFID technology in a variety of contexts for several years. For example, RFID technology has successfully been used to tag pharmaceutical products to reduce the risk of counterfeit medications use in the United Kingdom.

RFID is also proving to be very useful in identifying patients, increasing safety and reducing incidents of mistaken identity during critical surgery. It is being successfully used to locate patients needing extra care, such as the elderly, or patients suffering from Alzheimer's or memory loss.

Medical equipment is being more rapidly located and tracked within health-care facilities, leading to more effective use of resources. Waste management has been improved through the use of RFID.

11 See *Privacy Guidelines for RFID Information Systems* (June 2006), available at: **www.ipc.on.ca/images/Resources/up-rfidgdlines.pdf** and related materials at: **www.ipc.on.ca/index.asp?navid=67&fid1=16**

From a privacy point of view, the single most relevant consideration is whether and to what extent the RFID-related data collected or generated from the tags may be characterized as personally identifiable (health) information. To the extent that it is (or could be) personally identifiable data, then legal and regulatory privacy requirements are invoked.

For this reason, we have organized some of the known RFID technology deployments into three broad categories of increasing privacy relevance and concern:

1 Tagging things;

2 Tagging things linked to people; and

3 Tagging people.

Tagging *things*

RFID technologies have proven to be ideal for identifying and locating *things* because they increase the reading accuracy and visibility of tagged items far beyond bar codes and other labels. The results can include greater efficiency for automating inventory processes, finding misplaced items, and generally keeping better track of things as they move through their life-cycles.

Automatic identification remains the basis of all RFID information systems, but specific applications may be variously described as asset management, tracking, authenticity verification, matching, and process or access control, depending on the context and circumstances. Application types are not mutually exclusive: an implementation or deployment can combine elements of several application types. For example, RFID-based information systems that both identify *and* locate tagged items combine asset management with tracking (real-time or otherwise).

All of these application types are currently being used by health-care providers, many of which are large institutions with complex asset management and logistical requirements.

Sample RFID health-care deployment scenarios that involve the tagging of things include:

- Bulk pharmaceuticals;
- Inventory and assets (e.g., trolleys, wheelchairs, medical supplies);
- Medical equipment and instruments (e.g., infusion pumps, wheelchairs);
- Electronic IT devices (e.g., computers, printers, PDAs);
- Surgical parts (e.g., prosthetics, sponges);
- Books, documents, dossiers and files;
- Waste and bio-hazards management.

One of the key reasons for introducing RFID-based automatic identification technologies and systems is often to *improve operational efficiency*. The integration of RFID technology with business intelligence and analytics systems has proven the benefit of leveraging this technology for business process improvement.

RFID tagging and tracking of items has also been shown to save valuable staff time and costs associated with manual data collection and input (especially when it is routine and repetitive), and also with physical searches for misplaced or lost items. Further, RFID-tagged assets and items can help reduce human errors and mistakes, as well as improve auditability and accountability, resulting in better quality health-care services.

Efficiency gains may also be realized from more accurate and up-to-date inventory accounting, and from reduced "shrinkage" of valuable assets.

Many pharmaceutical RFID tracking and tracing initiatives are underway in the U.S., E.U., and Asia. Pharmaceutical "drug e-Pedigrees" have become the subject of considerable attention by the health-care and RFID industries, as well as by government health regulatory and licensing agencies across North America.

A drug pedigree is a statement of origin that identifies each prior sale, purchase or trade of a drug product, including the date of these transactions and the name and addresses of all parties to them.

The U.S. Food and Drug Administration (FDA) e-Pedigree requirements were outlined in a 1988 set of FDA regulations enacted following the passage of the Prescription Drug Marketing Act (PDMA) of 1987, created to address problems of drug counterfeiting in the pharmaceutical supply chain. Pharmaceuticals can travel through many different points in the distribution chain from the factory to a pharmacy or hospital, creating a significant counterfeit drugs issue. To address these issues and ascertain proper "chain of custody," the FDA has been investigating the use of RFID technology to increase supply chain security. At the time, the FDA anticipated that the e-Pedigree would be achievable by 2007.

The broad intent is to provide a documented chain of custody for high-value pharmaceuticals, from the production plant through to the dispensary, as well as the return and disposition of pharmaceutical items. In addition to automating the identification, documentation and pharmaceutical supply-chain management processes, drug pedigrees are also expected to help minimize incidence of counterfeiting and diversion, and to facilitate recalls.

Drug pedigree requirements can be fulfilled through traditional paper methods, but RFID technologies, combined with networked databases, offer a more automated, secure, and trusted way to establish such a pedigree.

Privacy Considerations

Generally speaking, the business of identifying and tracking inventory and objects does not involve collection, use or retention of personally-identifiable information. The uniquely identifying data stored on the RFID tags, which are read by interrogators, transmitted across networks, processed by middleware, stored in logs, shared with third parties, and acted upon in the context of relevant business processes, refers exclusively to "things" in a manner analogous to a product serial number. Accordingly, if there is no personally-identifiable health information, then privacy does not come into play.

In February 2004, the U.S. Food and Drug Administration recognized the potential of RFID information technologies to combat counterfeit pharmaceuticals and to provide more effective fulfillment of U.S.-mandated drug pedigree requirements.[12] In November 2004, the FDA issued a report recommending that drug makers use RFID to track bottles of the most commonly counterfeited drugs, with eventual extension to more drugs over time.[13] The FDA also published a guidance policy around the use of RFID in the pharmaceutical industry, which states, *inter alia* that:

- RFID tags are attached only to immediate containers, secondary packaging, shipping containers and/or pallets of drugs that are being placed into commerce;
- Drugs involved will be limited to prescription or over-the-counter finished products;
- RFID will be used only for inventory control, tracking and tracing of products, verification of shipment and receipt of such products, or finished product authentication;
- The tags will not contain or transmit information for the health-care practitioner or the consumer;
- The tags will not contain or transmit advertisements or information about product indications or off-label product uses.

The scope of the FDA's guidance makes clear that personally-identifiable information is not involved in the pharmaceutical supply chain management, and hence, privacy issues, do not come into play.

Examples of RFID Uses

The following examples provide a glimpse into the broad range of uses for which RFID technologies may be deployed by tagging things:

12 *COMBATING COUNTERFEIT DRUGS: A Report of the Food and Drug Administration* (February 18, 2004) available at: **www.fda.gov/oc/initiatives/counterfeit/report02_04.pdf**

13 Radiofrequency Identification Feasibility Studies and Pilot Programs for Drugs, Guidance for FDA Staff and Industry, Compliance Policy Guides, Sec.400.210, *Radiofrequency Identification Feasibility Studies and Pilot Programs for Drugs*, November 2004, available at: **www.fda.gov/oc/initiatives/counterfeit/rfid_cpg.html**

High Value Mobile Equipment: The ambulatory care centre of a large Boston-area hospital is using RFID to track and maintain more than 1,500 units of high-value mobile medical equipment, including wheelchairs, gurneys, portable oxygen tanks, intravenous (IV) pumps and defibrillators. The prices of these assets range from a few hundred dollars apiece to several thousand, and many of them, such as IV pumps and wheelchairs, need to be maintained on a regular schedule.

Cardiology Devices: A Detroit Medical Centre is installing an RFID deployment to track the institution's growing number of medical devices. The RFID solution will be deployed for the cardiology group. Fourteen RFID-enabled cabinets will be installed to store implantable stint devices. The goal is to streamline and automate the management of these devices. Time lost to the current manual processes will be recaptured, and the documentation of device usage and expiration will be made more accurate.

Infusion Pumps: A large health-care system in Georgia is deploying an RFID asset-tracking system to improve management and utilization of thousands of tagged infusion pumps and other high-value equipment.

Location Tracking: According to one RFID vendor, a large, multi-hospital health-care provider is installing a real-time location system that uses hybrid Radio Frequency tags, combined with infrared (IR), to pinpoint the exact room in which an asset is located. The health-care provider has performed a beta test of the RF-IR system in which each hospital room is fitted with a Room Locator, an IR transmitter designed to send a location-identifying code.

Surgical Sponges: An independent organization, "No Thing Left Behind," is halfway through clinical trials testing RFID-enabled sponges, interrogators and companion software, in surgical cases in five different medical centres across the United States. The No Thing Left Behind project's overall objective is to help hospitals, surgeons, perioperative care nurses, and patients work together to ensure that surgical tools used in an operation are never left inside a patient. Recent studies have estimated that cases of surgical objects left in patients occur in between one out of every 100 to one out of every 5,000 surgical procedures. Other studies have shown that two-thirds of all retained foreign bodies are surgical sponges.

Medical Waste: Hospitals deal with hazardous waste on a daily basis, so a comprehensive system is necessary to manage and dispose of it safely and efficiently. Usually outsourced to service providers, waste management is a matter of concern to many hospitals. They are unable to control the vendor's work processes and can't be certain if wastes will be handled in compliance with the work contract or local legislation. One RFID solution for waste management provides proof-of-delivery and receipt, as well as location tracking and activity records to ensure the integrity. Sealed waste containers are tagged with locked RFID bands that keep track of the container movements, ensuring that potentially hazardous waste is not

compromised en route to the waste management plant from the hospital. At the destination plant, the RFID bands automatically transmit information such as the arrival time, quantity and weight of waste back to the hospital for accountability.

Robotic Hospital Helpers: A Pittsburgh company has developed a hospital robot to perform such mundane but vital tasks as retrieving and delivering drugs and test specimens. Now, six of the more than 34 hospitals already using the robots are testing an RFID-enabled version, which carries an RFID interrogator used to locate RFID-tagged assets as it moves around a hospital. The robot finds its way around a hospital through the use of a facility map saved to its memory.

Guidance

Generally speaking, where there is no personally identifiable information collected or used by an RFID-based information system, and little likelihood or risk of RFID-generated data becoming personally identifiable information, then there are no privacy issues and, in Ontario, the provisions of *PHIPA* do not come into play.

In a similar manner, to the extent that pharmaceutical tagging and e-pedigree programs remain strictly a (bulk) supply-chain management issue, ending at the dispensary, the privacy implications are minimal, while the benefits may be considerable. The application of clear rules and guidance by regulatory agencies, such as by the FDA,[14] will help to provide additional assurance and confidence that privacy interests are not engaged.

Tagging things *linked to people*

The next class of RFID technology uses involve RFID tagging of items that are (or may be) linked to identifiable individuals and to personal information, usually on a more prolonged basis (ranging from one week in the case of tagged garments, to several years or longer in the case of patient dossiers).

Some RFID deployment scenarios that involve tagging things linked to *people* include:

- Medical equipment being used by patients, visitors or staff;
- Readers, tablets, mobile and other IT devices assigned to staff;
- Access cards assigned to staff or visitors;
- Smart cabinets;
- Devices, garments, or spaces (rooms) assigned to patients;
- Blood samples and other patient specimens;
- Patient files and dossiers; and
- Individual prescription vials.

14 For more FDA info and guidance, see **www.fda.gov/oc/initiatives/counterfeit/**

In each usage scenario, the main purpose of the tagging is to identify and track objects, as before, but the relative permanence of the tag, the nature and amount of the data collected, and the strength of the data's linkage to identifiable individuals may invoke privacy issues and concerns.

Privacy Considerations

Increasingly, RFID tags are being attached to items that are, or may be, linked to individuals. Privacy interests become progressively engaged with the strength and ease of this linkage, along with the sensitivity of the linked data. The same basic properties that make RFID information technologies and systems so useful for inventory control and supply management purposes can impact individual privacy when that tracking and control extends to individuals, especially when informed consent is lacking.

There are asset identification, tracking and management scenarios that could involve a link with personally identifiable information. For example: all touch-points or interactions with tagged items (and the data generated) by staff might be logged for audit and accountability purposes, engaging employee privacy interests. Tagged assets could also be temporarily assigned to individuals (beds, rooms, equipment) and, if they are mobile items, can become a proxy for tracking people through inference. Even if the data on an RFID tag is encrypted or otherwise unintelligible, the tag can still be used as a basis for tracking and its history correlated with personally identifiable information from another system. This could happen, for example, when use of an RFID-enabled visitor access card is correlated with a video capture of the bearer, at access points or other chokepoints.

Some RFID tags are re-writable and re-usable. If data about an individual, such as a patient identifier or drug prescription, is written locally to the tag, then it is possible it may be read and used in an unauthorized manner if it is not properly secured or destroyed.

If the RFID-tagged item *travels* with the individual, then extensive tracking and monitoring of the item is tantamount to tracking and surveillance of that individual. In the case of access cards, the threats and risks extend to hacking and cloning of the embedded RFID tags, allowing unauthorized individuals to effectively access secure spaces and to commit identity theft.

Unauthorized identification, tracking, surveillance, and profiling of individuals are very serious privacy issues. In addition, security issues related to RFID tags, including skimming, eavesdropping, interception, interference, tampering, cloning and misuse, can also impact individual privacy (as well as the operations of health-care providers).

As noted earlier (see "referential vs. non-referential systems"), RFID tags do not always contain personally identifiable information, such as a person's name. In most cases, they encode some semi-random unique alphanumeric string that can serve as a pointer, or index key, to a person's linked identifiable information, such as a medical or transaction record stored in a networked database (perhaps even transmitted offsite and controlled by third parties). RFID readers – often mobile – read tag data and use it to trigger an action, such as to display and record the tag contents, or to "look up" and retrieve (and use) data corresponding to the tag ID.

Readers themselves, or any RFID-enabled portable computing and communications device, may be assigned to health-care personnel to help them collect and transmit data stored on tags elsewhere. Usually this is intended to help staff accomplish their tasks faster and more efficiently, but the data collected can then be correlated with the personnel ID or role, and used to establish audit trails and to enhance accountability.

Generic (i.e., blank) RFID-embedded access cards may not serve as identity cards, yet their assignment to staff and permissible uses are controlled centrally. Typically, there is some linkage with identified individuals (i.e., the bearer), and all uses and attempted uses of the cards are routinely collected and retained in logs. This allows for the possibility of detailed profiles to be constructed.

Tagging patient specimens and other waste for proper handling or disposal may actually enhance privacy if the alternative involves labelling the item with human-readable personally-identifiable information or bar codes. As usual, much depends upon the strength of the linkage to the patient and the ease with which parties may make that connection (e.g., database access). In general, however, any tagged file or item that must be linkable to an individual, yet be passed around to multiple parties in a privacy-preserving manner (e.g., admission slip, test results, survey results/feedback, files, etc.), could potentially benefit from the deployment of RFID technology.

While the concern here is with the privacy and security issues related to RFID technologies, there will be very justifiable and defensible health-care-related reasons for deploying such technologies even where there are informational privacy implications. In these circumstances, it is important that the benefits be demonstrable, the privacy risks identified and properly mitigated, and the entire system developed and deployed in a transparent, and responsible manner.

Examples of RFID Uses

The following deployment examples provide a glimpse into the broad range of uses for which RFID technologies for tagging things linked to people may be deployed:

Hand-washing compliance: To reduce the spread of infections, a new automated hand-sanitizing system uses RFID to monitor how well health-care workers wash their hands. The wash cycle automatically starts when the caregiver's hands are inserted into the machine's cylindrical openings. Health-care-associated infections affect nearly 2 million individuals annually in the U.S., and are responsible for approximately 80,000 deaths each year, according to a guide published by the Centers for Disease Control and Prevention (CDC), in collaboration with the Infectious Disease Society of America (IDSA) and the Society of Healthcare Epidemiology of America (SHEA). The transmission of health-care-related pathogens most often occurs via the contaminated hands of health-care workers. When washing hands, a caregiver wearing an RFID badge is identified by the machine's RFID interrogator. The device records the date and time, as well as the beginning and end of the wash cycle, then communicates that information to the database. If a caregiver removes the hands before the 10-second cycle finishes, the interrogator transmits this information to the back-end database. Hospital administrators can then run departmental statistics and other compliance reports to determine which caregivers have completed the washing cycles.

Smart Cabinets: Texas University Medical Center researchers are using RFID to manage the supply of chemicals and other materials used in biology research. The Center has installed two storage cabinets fitted with RFID interrogators. Items stored inside the cabinets are fitted with RFID tags. Every authorized researcher at the university has been issued a credit card-sized RFID key card carrying a unique six-digit ID number that is used to release the lock. The interrogator reads the key card's ID number and the item tags in the cabinet before and after it has been opened, enabling the software application to calculate what has been removed, and to update the online inventory data. This information is accessible via the Web by university administrators, researchers and suppliers, and generates e-mail messages to the school's accounts payable department and to the person who removed the items. Besides recording each transaction, the system helps suppliers know immediately what supplies have been used, what needs to be paid for and what needs replacing.

Specimens: A well-known medical practice with diagnosis and treatment facilities scattered across the U.S. piloted an RFID system to allow medical practitioners to better manage specimens of patient tissue. Deployed at endoscopy facilities, the tissue samples are tagged and tracked from the moment they are collected until they are delivered to the pathology laboratory for analysis, a series of steps characterized as "crucial." The pilot lasted five months, and the demonstrable benefits included accurate data communication and verification, as well as improved efficiencies in specimen management. The plan now is to rapidly phase in an expansion of the pilot.

Blood bags: In Malaysia, the government and three medical institutions are testing an RFID system for tracking blood bags, with the ultimate goal of eventually equipping more than 300 other government and private hospitals and clinics. The system combines blood bag tagging with smart cabinets to enable automated, efficient track-and-trace visibility. Eventually the system could manage Malaysia's entire blood bank, which includes 500,000 transfusions annually. The expected benefits include improved blood bag identification, inventorying, and logistics. Cross-matching, in which a recipient's blood type is matched to available donated blood, will be streamlined. Internal blood management processes will be made more efficient. Blood stock will be better maintained. Errors, blood-type mismatches, and waiting times will be reduced. Data management and access overall will improve, including easy report generation for inventory, donation history, and donor/patient profiles. Registration and results screening during the blood donation processes will be simplified. Lastly, the system will enable analytics for the entire blood bank management process.

Medicine Dispensing: A Southeast Asian RFID systems provider has introduced RFID-enabled products designed to help health-care providers track pharmaceuticals and monitor drug administration, to make sure that correct doses are given. The company's intelligent medicine-dispensing system combines RFID tags and readers, workflow software, electronic medical records (EMRs), and a central database in an integrated solution. This enables nurses and doctors to view patient records, update them in real-time, and double-check prescription dosages at the moment they administer them. The system can also automatically send prescriptions to pharmacists.

Patient Files: An acute-care and teaching hospital in New Jersey is implementing an RFID-enabled patient record management solution. Seeking both increased efficiency and compliance with *Health Insurance Portability and Accountability Act (HIPAA)* (which places heightened importance on patient information management), the hospital has targeted its Sleep Centres, which provide comprehensive evaluation and treatment for patients experiencing sleep-related problems. The centres manage 5,000 patient files. Each file is tagged with an RFID tag, allowing it to be tracked from the moment it is created for a new patient until the file is retained in storage. RFID readers are positioned in key locations around the centre to enable automatic tracking and encoding of the tags as they are moved from one place to another. Reads and writes to the tags are dynamically updated in the central database, ensuring real-time, accurate location data. The centres also have a series of handheld readers for routine inventory and locating misplaced files.

Handheld Devices to Verify Medications: The St. Clair Hospital in Pittsburgh developed and implemented an RFID-based system to help protect patients from medication errors and reduce health-care costs. Using bar code and RFID technology and a wireless network combined with HP iPAQ Pocket PCs, the VeriScan medication administration verification system confirms that a nurse has the correct patient,

medication, time, dose and route each time a medication is administered. The system has been in use for two years and is preventing more than 5,000 medication errors yearly, according to the hospital's chief operating officer. "With close to 1.3 million doses dispensed each year from St. Clair Hospital's pharmacy, we have plenty of opportunities for medication errors." The RFID system helps the hospital nursing staff avoid most of those errors and the associated costs, with estimated costs savings of more than $500,000 annually. When it comes time to administer a medication, the nurse uses an HP iPAQ Pocket PC to scan bar codes on the medication package and RFID tags on the patient's wristband. The VeriScan software compares the two sets of patient and medication data and alerts the nurse to any discrepancies. New orders, changes to orders and discontinued orders are available in real-time so that the nurse is aware of medication changes without delay. Not only does patient information pop up on the handheld display screen, but also a picture of the patient, which was taken when the patient was admitted. The device records the date and time the tags and bar codes are read, and then wirelessly sends all the data (bar codes, RFID tag numbers, and timestamp) to the database, where it is compared with the doctor's latest orders. Voice commands on the handheld announce, "Patient identification confirmed," or, in the case of discrepancies, "Access denied." In addition, any new medication orders, order changes or cancellations are automatically downloaded so that nurses can learn about them immediately.

Pharmaceutical tagging (item-level): While most industry efforts are directed at realizing the benefits of tagging and tracing bulk pharmaceuticals in the supply chain, as discussed earlier, a smaller subset of initiatives is investigating the benefits of tagging item-level drugs, or even individual prescriptions, usually in more limited health-care provider contexts.

As noted in some of the case studies above, health-care providers are seeing merit in tagging and tracking specific drugs within their own care environments, principally to reduce patient medication errors and also to maintain accurate inventory records. Using RFID technology, specific drugs may become associated with patients and staff in the course of their use, helping to provide an accountable and auditable record.

More ambitious RFID pilot projects involve integrating the technology into medication packaging for monitoring, patient diary and reminding purposes. In these cases, RFID technologies serve as an automated mechanism for ensuring that patients are taking the correct drugs, in the right dose, at the right times, perhaps for clinical testing and recording purposes. The informed prior consent of the patient is critical in such scenarios.

Less clear is the extent to which prescription vials provided directly to individuals by pharmacies are currently being RFID-tagged (for example, to help track and speed up refills). This use case scenario presents the strongest privacy issues, i.e., the

possibility that individuals may carry on their persons RFID tags containing sensitive prescription information that could be scanned and read by unauthorized parties.

Patients have a legitimate right to know how easy it would be for unauthorized parties to scan and read the contents of personal prescription vials carried in a purse or pocket, and to be given a non-RFID alternative choice. Personal health information that may be inferred from the drugs a person takes is highly sensitive, and requires strict controls and assurances against unauthorized disclosure and collection. Efficiency and convenience should never automatically trump privacy interests!

Guidance
To the extent that personal information is involved and potentially at risk, we urge moving forward with caution, diligence, and a comprehensive information governance program. When assessing the extent of personally identifiable information involved and the degree of risk involved, the following important questions should be asked regarding the system design and information flows:

- Whether personal information is stored on the tags;
- Whether the tagged items are considered personal;
- The likelihood that the tag will be in the proximity of compatible unauthorized readers;
- The length of time records are retained in analytic or archival systems; and
- The effectiveness of RFID security controls, in particular:
    - The efficacy of tag memory access control and authentication mechanisms;
    - The ability of tags to be disabled after use; and
    - The ability of users to effectively shield tags to prevent unauthorized reading.

Prescription tagging: If and when RFID tags are affixed to individually prescribed vials, pharmacies and health-care providers will have to address a number of privacy questions and concerns:

- Objective of tagging vials – are they clearly defined? Combating pharmaceutical counterfeiting, fraud and diversion are less compelling reasons at the individual prescription level.

- An account of any (new) information vulnerabilities and threats, and appropriate countermeasures to mitigate them. How easy is it for others to read and understand the contents of the tagged vials? Can these vulnerabilities be addressed through information security measures, such as encryption or shielding, and through better patient education?

- Do your privacy policies and procedures extend to the handling of RFID-tagged vials? Do they cover any potential use or misuses of the tag and its data?

Tagging *people*

The third and final class of RFID uses involves the intentional tagging and identification of individuals, rather than the devices, tokens or other assets they may be carrying or associated with. The distinction can be subtle since, technically speaking, it is always the tag that is identified in any RFID systems. However, when we talk about tagging people, we are focusing on the primary purpose of the RFID deployment in question, as well as the relative strength and permanence of the linkage of the tag to the individual and his or her personal information.

For example, we would *exclude* from this category a generic or reprogrammable RFID-enabled access card that is temporarily signed out for use by an employee, contractor or visitor. The primary purpose of the card is to authorize physical access to certain facilities or spaces, rather than identifying the bearer. The card assignment may be temporary in nature, and the card contains no specific personally identifiable information embedded or on its face. Any linkage of the card ID to the individual is retained only in a central register rather than for operational use. Someone else may use the access card at a later date.

Examples of RFID used (or intended to be used) to identify and track individuals in health care contexts include:

- Health-care employee identification cards;
- Patient health care identification cards;
- Ankle and wrist identification bracelets (e.g., for patients, babies, wandering or elderly patients); and
- Implantable RFID chips.

The assignment of temporary RFID-enabled bracelets or anklets to patients for the duration of their hospitalization and treatment, especially in large facilities, can help reduce the risk of patient misidentification, wandering or treatment error.

RFID-enabled bracelets are being effectively used by many hospitals and health-care facilities as alternatives to printed bar code identification to securely identify patients. Consent is typically provided or implicit, in the same manner as would be provided to allow identification through the use of a bar code or human readable tags.

The practice of assigning RFID-enabled bracelets to newborn babies, in order to prevent inadvertent mix-ups or abduction, is considered to be a reasonable, proportional and effective measure. One such maternity identification program also assigns a matching RFID to the mother, for added assurance, in order to confirm the match between mother and child.

In many cases, the use of RFID wristbands, surprisingly, offers better patient privacy due to the fact that confidential and often sensitive medical information can be securely stored in the RFID tag, or accessed automatically from a centralized system rather than printed in human-readable format on the band itself.

Other examples include tracking medical researchers who work with bio-hazardous and contagious materials, where records of all movements and interactions are imperative.

RFID-embedded ("contactless") identification cards are a special category of health-care RFID use. Here we must distinguish between employee identification (and access) cards (whether "smart" or not), and patient identification cards. Employee Identification cards are increasingly being equipped with RFID technologies in order to identify and authenticate the bearer and facilitate access to physical spaces and other (e.g., computer) resources, as well as for process control and audit purposes. Dual or multi-purpose employee identity cards can serve differing functions at different times, according to context. Such a multi-purpose card and the data it contains, if not properly controlled, invites over-identification for some functions, function creep, and unwanted employee profiling.

Patient identification cards are used by health-care facilities to facilitate patient admission, treatment, and record-keeping. Given that personal health information is highly sensitive, significant security and privacy concerns would need to be addressed. The value of the embedded RFID data, if cloned, could be especially high since it may be easily obtained by stealth and used to obtain free health care by anyone capable of cloning the card's contents (or acquiring a cloned card). This could open the door to identity fraud and theft.

Perhaps the most controversial use of RFID for tracking people involves implanting small RFID chips inside human bodies, typically below the skin of the upper arm. Approved by the U.S. Food and Drug Administration in 2004, RFID implants are being trialled in a number of non-medical scenarios, including military, employment, financial and recreational. In the health-care realm, voluntary RFID implant programs exist for individuals wishing to allow automatic identification and retrieval of their medical records by virtue of a 16-digit number correlated to information stored on a secure database. New RFID-based implants can also act as biosensors and as micro electro-mechanical systems for monitoring health conditions.

Generally speaking, if an RFID patient identification program responds to a defined problem or issue in a limited, proportional and effective manner, and is deployed in a way that minimizes privacy and security risks, at least as effectively as any alternative solution, then in principle there should be few privacy concerns with the program.

Privacy Considerations

Few topics elicit such strong views among the privacy community, medical practitioners, ethicists, consumer and civil rights groups, technologists, and public policy and lawmakers than proposals for using any type of technology to automatically and remotely identify and track human beings without their consent.

The prospect of remote, automated identification and tracking of individuals goes straight to the heart of critical privacy fears and concerns about RFID technology. These fears include:

- Surreptitious identification of individuals by known and unknown parties, without their prior knowledge or consent;
- Systemic tracking and surveillance of individuals by known and unknown parties, without prior knowledge or consent;
- The construction of histories and profiles about individuals and their interactions, without the individual's prior knowledge or consent;
- Correlation of acquired data with contextual and other information obtained elsewhere;
- Unwanted or incorrect inferences about the individual derived from the data;
- Unauthorized revelation of personal and private facts and disclosure to others;
- The inherent imbalance of power and potential for undesirable social engineering, control and discrimination on the basis of RFID-generated data;
- Unauthorized access, theft, and loss of RFID-based personal data held by custodians;
- Unauthorized interception and access to protected information stores by unknown parties, due to poor information security practices;
- The cloning of RFID identification data and possibility of unauthorized access to physical and logical resources, and of identity theft;
- The negative consequences upon the individual of all the above activities;
- The inability of individuals to find out about the collection and misuse of their data, and to remedy any errors or abuses; and
- The lack of confidence and trust by individuals in the information management practices of organizations.

More than two dozen U.S. states have, in the past two years, introduced bills intended to specifically restrict or otherwise prescribe the use of RFID for human identification and tracking.

At least three states have enacted laws to ban mandatory RFID "chipping" of individuals. Highly contentious public proposals for large-scale RFID-enabled passports, travel documents, enhanced driver's licences and other portable documents continue to be actively debated, with privacy concerns at the forefront.

It is interesting to note the complexity and contentiousness of the matter for civil society. Few of these proposals, however, deal with health-care scenarios. One major exception is the subcutaneous "chipping" of patients, such as for long-term care patients suffering from Alzheimer's or dementia, who may be incapable of reliably identifying themselves for proper care and treatment, and are prone to wandering.

The practice of subcutaneous chipping has been approved by the U.S. Food and Drug Administration as safe, and at least one U.S. company offers a nationwide program for individuals to voluntarily become chipped in order to be identified faster by participating caregivers, especially if unconscious or otherwise unable to communicate. The chip contains a short alphanumeric string that, when queried against a secure database, allows rapid access to personally-stored health records.

The U.S. Council on Ethical and Judicial Affairs (CEJA), which develops policies for the American Medical Association, issued a report (2007) saying that implantable RFID devices may compromise people's privacy and security because it is yet to be demonstrated that the information in the tags can be properly protected.

Complex legal and ethical questions are invoked by RFID (and other ICT) implants in the human body. Many of these questions were addressed by the European Group on Ethics (EGE) in Science and Technology to the European Commission. In its 2005 report, the EGE stressed that RFID (and other implants) in the human body can have repercussions for human dignity, and that their use for health-care requires informed consent, utmost transparency and strict limits in the case of patients unable to consent. Implants to gain control over the will of people should be banned, and the autonomy of the patient is the yardstick.

Apart from subcutaneous chipping of the hospitalized elderly, there may be other justifiable reasons and circumstances for using RFID technologies in a less-invasive and less-permanent manner, to identify staff and patients. At least one elderly-care treatment centre assigns the elderly an active tag on a lanyard, allowing staff to automatically monitor and track the location of patients as they move about the facilities, and to respond immediately in the event of an incident.

Examples of RFID Uses

Patient ID system: In January 2007, HP and Precision Dynamics Corporation (PDC) announced the deployment of a comprehensive RFID-based patient management system at the Chang-Gung Memorial Hospital (CGMH) in Taiwan. The system offers the medical facility numerous benefits and has already realized positive results in patient identification. Patients are given wristbands with embedded RFID chips that increase the accuracy of patient identification and decrease the risk of so-called “wrong-site” and “wrong-patient” surgery, in which the incorrect operation is performed on the correct patient, or the correct operation is performed on the incorrect patient. Under the new system, CGMH has realized 100% accurate patient identification in the operating room. The system also automates data gathering, which cuts down on previous human error resulting from oral communication and manual data entry. This automation also yields better compliance with standard operating procedures. Alerts are generated in real-time when the sequence of a prescribed process is going amiss. In addition to improved accuracy, the HP-PDC

system brings improved efficiency. Medical staff now spend 4.3 minutes less verifying patient data per incident. This figure multiplied across hundreds or even thousands of daily patients (CGMH is part of an 8,800-bed health-care system) can bring dramatic savings and, ultimately, better health care. Lastly, the RFID wristbands offer better patient privacy in that the confidential and often sensitive medical information is stored on the RFID chip rather than printed in plain view on a wristband.

Wi-Fi Elderly Care: An Australian provider of elderly care is using a Wi-Fi-based RFID system to enable residents to quickly and easily call for help when they need it. The medical alerting system notifies caregivers any time a resident wanders into a dangerous area or hasn't moved for a long time, indicating that they may need help. Affixed to lanyards that can be worn around the neck, the tags measure approximately 2 by 1.5 inches and are a half-inch thick. They are water-resistant and feature large, easy-to-find call buttons that residents can press when they are in trouble or need assistance. Staff also wear the tags so they can easily issue an emergency alert. When a tag's call button is pressed, the tag transmits its unique ID number to a nearby Wi-Fi access point, which passes that information on to each staff member's mobile handheld device, as well as to flat-screen monitors installed throughout the complex. The system can identify the room in which a tag is located, and includes a set of configurable rules designed to trigger alerts when broken.

Patient Monitoring: A Belgian University Hospital may be the first to use RFID technology not just to track where patients are, but how they are. The hospital is using Wi-Fi RTLS tags integrated with medical monitoring equipment to remotely transmit patient health data and emergency alerts. Nurses carrying wireless phones can instantly access patient information from the monitoring equipment, including blood pressure, oxygen level, and even electrocardiogram images. In case of emergency, the RTLS tags can automatically issue an alert. The system is currently being deployed at a 1,100-bed hospital. The integrated system includes the hospital's legacy Wi-Fi wireless network, Wi-Fi-enabled RTLS tags, wireless phones, a Wireless Location Appliance, various communication technologies, and monitoring equipment from a major medical systems manufacturer. The tags are placed on monitoring equipment assigned to cardiology patients, who are then free to take strolls, visit lounges, and move about the facility. The application will provide patient location data in addition to advanced medical telematics information.

Protecting Newborns: Each year in the U.S., there are 100 to 150 baby abductions, with more than 50% of those babies taken from health-care facilities. There are also over 20,000 mix-ups, with the majority caught before the parents even know. A Dallas hospital was the first hospital to implement the "Hugs and Kisses" RFID system, which uses active RFID tags to tag babies and mothers. A "Hugs" tag is attached to the baby's foot. Mothers wear a "Kisses" wrist band. If they pick up the wrong baby, they hear an audible alarm, while picking up the correct baby results in

a confirmation. RFID reader installations mean that any attempted abduction is detected as the baby is moved, with the system linked to CCTV and security. The tags are disabled after a time lock when the fire alarm has been activated. Over 400 U.S. hospitals are currently using the RFID-based baby and mother monitoring system.

Medical Implant: Doctors at the University of Texas Southwestern Medical Center, working with engineers from the University of Texas, Arlington, have developed innovative RFID-based medical technology to detect gastroesophageal reflux disease, caused by stomach contents moving up the esophagus. The condition, commonly referred to as esophageal reflux or GERD, is estimated to affect as many as 19 million people. The new solution combines RFID with sensor technology to measure and transmit data from within a patient's body. A dime-sized RFID chip is inserted into the esophagus, where it remains pinned until a physician removes it. Equipped with an electrical impulse sensor, the chip measures particular impulses that indicate the presence of acidic or non-acidic liquids in the esophagus. These collected measurements are transferred from the RFID chip to a wireless receptor hanging around the patient's neck.

Implants: In September, VeriChip Corporation, a provider of RFID systems for health care and patient-related needs, announced that more than 90 Alzheimer's patients and caregivers received the VeriMed™ RFID implantable microchip at the official launch of their Project with Alzheimer's Community Care. VeriChip's collaboration with Alzheimer's Community Care consists of a voluntary, two-year, 200-patient trial to evaluate the effectiveness of the VeriMed™ Patient Identification System in managing the records of Alzheimer's patients and their caregivers.

Guidance

Because RFID technology allows for the automatic identification of identifiable individuals, special vigilance is required when tagging people. The privacy and security risks associated with collecting, processing, and retaining personal information are the greatest here, and require the strictest, most rigorous and most transparent application of project management skills and risk mitigation measures.

Subcutaneous RFID chips appear to be the most extreme form of using RFID technology to identify humans with its inherent risks. The majority of deployments, however, involve the simple assigning of an RFID-embedded card or bracelet to an individual. When pursuing this type of identification purpose, the following important design parameters should be considered:

- Whether the RFID tags will directly encode personally identifiable information, or serve as pointers to PII stored elsewhere;
- Whether the tags and their data will be part of an "open-loop" system (i.e., involving multiple organizations and actors);

- Whether the data will be stored or controlled by outside third parties;
- Whether and to what extent the tags are vulnerable to tampering and cloning;
- Whether and to what extent the tag and its contents will be under the control of the individual;
- Whether the tags will be active or passive, read-only or re-writable;
- Whether the tag is temporary or otherwise removable from the individual (e.g., bracelets, anklets, lanyards, implants, ID or namecard or other token); and
- Whether the tag's unique data, or tag itself, will be permanently destroyed once its use expires.

Professional and Ethical Considerations

Whenever considering, designing and implementing information systems that involve collecting, using, retaining and disclosing sensitive personal (health) information of patients, health-care providers are strongly advised to consult appropriate professional codes and other codes of ethics. When in doubt, always check with additional sources.

In Canada, many such policies, guidelines and codes for the ethical uses of health information have been developed and are readily available. Readers are encouraged to visit the following useful websites:

- Canadian Institute for Health Research (CIHR): Policies and Guidelines in Ethics at: **www.cihr-irsc.gc.ca/e/29335.html**
- Developing a quality criteria framework for patient decision aids: online international Delphi consensus process at: **www.bmj.com/cgi/content/full/333/7565/417**
- Ethics in Mental Health Research at: **www.emhr.net/ethics.htm**

Conclusions

In this paper, we have described RFID technology, provided examples of current uses, and discussed its suitability for the health-care sector. RFID offers many potential benefits in a wide variety of health-care contexts for improving the safety, efficiency and effectiveness of health-care delivery. However, if not implemented with due care, it can also impact privacy interests in profound and negative ways.

We have grouped together three different classes of RFID deployment and described, at a general level, some of the security and privacy issues that could arise. We have suggested the use of various privacy-enhancing methodologies, tools, and techniques intended to ensure that privacy safeguards are built into information systems from the very start, sufficient to mitigate known vulnerabilities, threats and risks. The resulting RFID systems should merit the confidence and trust of all users and stakeholders, as well as meeting legislative compliance requirements.

The first class of RFID use involves the tagging of "things" alone, with no linkage to personal identifiers and, accordingly, no privacy issues.

The second class involves the *potential* for data linkage to personal identifiers, raising the possibility that individuals could be identified and tracked. This calls for the introduction of strong privacy-protective measures to ensure that no unintended consequences arise.

The third class involves the use of RFID intended precisely for the purpose of identifying people, thus serving as personal identifiers. While strong privacy measures are clearly required here, the concern with unintended consequences in this category is arguably less than in the previous one, where data linkage with personal identifiers is ancillary to the primary purpose. Care must always be taken, however, regardless of the extent of the threat posed, for strong protection of privacy.

We must ensure that Fair Information Practices – the heart of privacy and data protection – are clearly understood and implemented. Doing so invariably paves the way to preserving our privacy.

The authors gratefully acknowledge the work of Fred Carter, Senior Policy & Technology Advisor, Office of the Information and Privacy Commissioner of Ontario, and the HP Canada Emerging Technologies Team in the preparation of this paper.

RFID Resources

RFID Technology Information Sources

- *RFID Applications, Security, and Privacy,* Garfinkel & Rosenberg, eds. 2006.
- HP Global issue Brief – Radio Frequency Identification (RFID): **www.hp.com/hpinfo/abouthp/government/ww/gib_rfid.html?jumpid=reg_R1002_USENTBC**
- GS1 EPCglobal:
  - GS1: **www.gs1.org**
  - EPCglobal: **www.epcglobalinc.org**
  - Discover RFID: **www.discoverrfid.org**
- RFID Journal: **www.rfidjournal.com**
- RFID Update: **www.rfidupdate.com**

RFID & Health Care/Life Sciences

- RFID Journal, *Radio Frequency Identification in Health Care* (Dec 2007), at: **www.rfidjournal.com/article/articleview/3777**
- Informationsforum RFID, *RFID for the Healthcare Sector* (August 2007), at: **www.info-rfid.de/downloads/RFID_-_for_the_Healthcare_Sector.pdf**
- The European Group on Ethics in Science and New Technologies to the European Commission, *Opinion 20: Ethical aspects of ICT implants in the human body* (2006)
  Press Release: **http://ec.europa.eu/european_group_ethics/docs/cp20_en.pdf**
  Report: **http://ec.europa.eu/european_group_ethics/docs/avis20compl_en.pdf**
  - *The ethical aspects of ICT implants in the human body: Proceedings of the Roundtable Debate* (Amsterdam, 21 December 2004) at: http://ec.europa.eu/european_group_ethics/publications/docs/tb21dec_ict_en.pdf.
- AMA Council on Ethical and Judicial Affairs, CEJA Report 5-A-07: *Ethics Code for RFID Chip Implants* (July 2007) at:
  www.ama-assn.org/ama1/pub/upload/mm/467/ceja5a07.doc
- IDTech Ex, *RFID for Healthcare and Pharmaceuticals 2007-2017*, at:
  www.idtechex.com/products/en/view.asp?productcategoryid=101

RFID & Privacy

- Office of the Information and Privacy Commissioner (IPC) of Ontario (Ann Cavoukian, Ph.D.), **www.ipc.on.ca**
  - *Tag, You're It: Privacy Implications of RFID Technology* (2004)
  - Overview of RFID Privacy-Related Issues (2006), Presentation by the Commissioner to EPCglobal Inc (July 2006), at:
    www.ipc.on.ca/images/Resources/up-2006_07_20_IPC_EPCglobal.pdf

- Can You Read Me Now? The Privacy Implications of RFID (March 2007), speech to the International Association of Privacy Professionals/-KnowledgeNet Toronto on the privacy implications of RFID technology, at: **www.ipc.on.ca/images/Resources/up-12007_03_13_IAPP_KnowledgeNet.pdf**

- RFID and Privacy: A Public Information Center: **http://rfidprivacy.mit.edu/access/happening_legislation.html**

RFID Use Guidance

- IPC, *Commissioner Cavoukian issues RFID Guidelines aimed at protecting privacy*, News Release (June 2006) **www.ipc.on.ca/images/Resources/up-2006_06_19rfid.pdf**
  - Privacy Guidelines for RFID Information Systems (RFID Privacy Guidelines) **www.ipc.on.ca/images/Resources/up-1rfidgdlines.pdf**
  - Practical Tips for Implementing RFID Guidelines **www.ipc.on.ca/images/Resources/up-rfidtips.pdf**

- Article 29 Data Protection Working Party, *Results of the Public Consultation on Article 29 Working Document 105 on Data Protection Issues Related to RFID Technology* (June, 2005) at: **http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp111_en.pdf**

- Article 29 Data Protection Working Party, *Working document on data protection issues related to RFID technology* 10107/05/EN WP105 (January 19, 2005) at: **http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf**

- European Commission, *Radio Frequency Identification (RFID) in Europe: steps towards a policy framework* {SEC(2007) 312}(March 2007), at: **http://eur-lex.europa.eu/LexUriServ/site/en/com/2007/com2007_0096en01.pdf**

- European Data Protection Supervisor, Opinion on "RFID in Europe … steps towards a policy framework" (Dec 2007), at: **www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2007/07-12-20_RFID_EN.pdf**

- European Parliament Scientific Technology Options Assessment (STOA), *RFID and Identity Management in Everyday Life: Striking the balance between convenience, choice and control*, IPOL/A/STOA/2006-22 (July 2007) at: **www.europarl.europa.eu/stoa/publications/studies/stoa182_en.pdf**

- Electronic Privacy Information Center (EPIC), *Privacy Implications of RFID Technology in Health Care Settings* presentation to the U.S. Department of Health & Human Services (2005), at: **www.epic.org/privacy/rfid/rfid_ncvhs1_05.ppt**

- Conference of International Privacy and Data Protection Commissioners, *Resolution on Radio-Frequency Identification* (2003) at: **www.privacyconference2003.org/resolutions/res5.DOC**
- U.S. Federal Trade Commission, *Radio Frequency Identification: Applications and Implications for Consumers* (Workshop Report, Mar 2005) available at: **www.ftc.gov/os/2005/03/050308rfidrpt.pdf**
- CDT Working Group on *RFID: Privacy Best Practices for Deployment of RFID Technology*, at: **www.cdt.org/privacy/20060501rfid-best-practices.php**
- RFID Position Statement of Consumer Privacy and Civil Liberties Organizations, at: **www.privacyrights.org/ar/RFIDposition.htm**
- Halamka, Juels, Stubblefield, and Westhues, The Security Implications of VeriChip Cloning, at: **www.jamia.org/cgi/content/abstract/M2143v1**

RFID & Security

- National Institute of Standards and Technology (NIST), *Guidelines for Securing Radio Frequency Identification (RFID) Systems Recommendations of the National Institute of Standards and Technology* (April 2007), Special Publication 800-98 at: **http://csrc.nist.gov/publications/nistpubs/800-98/SP800-98_RFID-2007.pdf**
- RSA Laboratories, RFID Privacy & Security, at: **www.rsa.com/rsalabs/node.asp?id=2115**
- Demo: Cloning the Verichip, at: **http://cq.cx/verichip.plRSA**. Laboratories, RFID Privacy & Security, at: **www.rsa.com/rsalabs/node.asp?id=2115**
- "Security Analysis of a Cryptographically-Enabled RFID Device" at: **www.usenix.org/events/sec05/tech/bono/bono.pdf**
  Privacy-Enhancing Technology (PET) Award Press Release at: **www.microsoft.com/emea/presscentre/pressreleases/20062007PETawardsTS.mspx**