Privacy Systems in Smart Spaces

Jamil Al-Jabi, Jamal Abu Rrub, Khalil El-Khatib
Business and Information Technology
University of Ontario, Institute of Technology
Oshawa, Canada
{jamil.al-jabi, jamal.aburrub, khalil.el-khatib}@uoit.ca

ABSTRACT: *Radio Frequency Identification (RFID) systems are used to automatically identify objects by using radio waves transmitted between readers and tagged objects. While the RFID technology has numerous potential applications in healthcare, military, commerce, to list a few, it raises many security and privacy risks and concerns due to the wireless transmission for data between the tag and the reader. Additionally, the limited computational power of the tag is usually insufficient to apply robust security measure.. In this paper, we will discuss the main RFID privacy and security threats and their countermeasures. Our emphasis will be on RFID usages in smart spaces such as smart hospitals and how to maintain the privacy of subjects in the systems including doctors, nurses and patients.*

Keywords: RFID, RFID Privacy, Healthcare, Securty Risk, Privacy Risks

Received: September 2011, Revised 9 November 2011, Accepted 17 November 2011

1. Introduction

Identification plays major function in our lives, ranging from simple basic daily tasks to business operations. Examples include: barcode technology for identifying items such as groceries, vehicle Identification Number (VIN) for recognizing vehicles, magnetic strip cards used for payment methods like credit cards, and biometric traits for identifying humans, to list a few. Among identification systems are the automatic identification related to the methods of identifying objects and collecting their data automatically. Immediate identification of people, animals, goods and products became essential for quicker and better services especially in our current age of technology [1].

Over the last few years, Radio Frequency Identification (RFID) technology has been successfully used for automatic identification, and has been deployed in almost unlimited number of applications and methods. However there are a number of concerns that have been raised related to potential privacy implications linked to the implementation schemes of RFID technology such as tracking and profiling tagged people or tagged objects related to people. Privacy advocates have been calling for solutions that can provide identification without sacrificing privacy; these solutions should allow tracking tags attached to people, while providing mechanisms for protection against unauthorized surveillance and tracking.

In the following sections, we will review the current challenges with RFID technology related to privacy protection, we will also list down some of the proposed solutions to overcome the privacy concerns and obstacles facing the deployment and adoption of this technology in smart places such as smart hospitals.

2. RFID Operating Principles and Fundamentals

RIFD technology uses radio frequency signals for wireless date exchange between a reader and an RFID tag from a distance without the need of direct contact. It is used for automatic identification and to trigger data collection or automation of processes. A typical RFID system consists of few readers (transceivers) either mobile or stationary, tags (transponders) that are attached to objects to be identified, and middleware or a back-end database. The identification of RFID tag takes place by the reader over the wireless medium or air to transfer or receive information stored on the tag. This information is usually combined with other contextual information stored on a back-end database [1].

2.1 RFID Tags

RFID tags are used to uniquely identify individual items or objects; they are made of small electronic components. Although RFID tags come in different shapes and styles, all RFID tags must have the following components: Tag Antenna, Integrated Circuit and Substrate.

There are two general classes of RFID tags: passive and active. Passive tags have no internal power source, and the signal from the interrogating reader is used to power the tag; they can only work within few meters ranges (short ranges). The new generation of battery-assisted passive tags can hold larger amount of data and can transmit over longer distance. Active tags on the other hand are using battery power for transmission and maintaining their internal state; although they are more expensive than passive tags, they can operate and initiate communication over long ranges. Active tags provide additional functionality over passive tags, including the ability to integrate sensors (e.g. tamper, motion, temperature detection sensors, etc.) and can hold larger amount of data. All RFID-tag classes have frequencies that can vary from Low, High, and Ultra-High; they are controlled by market standards such as ISO and Electronic Product Code (EPC) [2].

2.2 RFID Reader

An RFID reader is composed of two major components: a microprocessor and an antenna. It communicates with tag by transmitting and receiving Radio Frequency (RF) waves. It also provides an interface for RFID application software to access the data stored on tags.

2.3 RFID Middleware

An RFID middleware is the software component between the RFID reader and the application software. Its main function is to translate the low-level RFID hardware communication with the tag into context event information to enable further processing by the software application.

3. RFID Applications in an Integrated Healthcare Environment

RFID is an evolving technology that can be utilized within healthcare applications and institutions to help in validating the existing process and improving medical procedures, equipments utilization, allocation and tracking. It can be integrated into process controls in order to reduce operating cost, minimize human errors and mistakes to improve medical services and patients' safety. Using the RFID technology as a part of a hospital daily operation will create an environment we dubbed as smart hospital environment. In this section we will provide some medical applications that can benefit from the RFID technology in order to improve the process control and productivity within a smart hospital.

3.1 Equipment Location Tracking

RFID technology has been extensively used for inventory management, and can potentially be used effectively in healthcare environment to track equipment, for inventory status, as well as for unit level usage and availability. . RFID system can reduce the time wasted by staff looking for a specific equipment and therefore increase the staff effectiveness as they are able to focus on their primary job activities instead of looking for needed equipment. In addition the amount of unfound equipment will dramatically be reduced which will result in avoiding the possession of unnecessary backup or standby equipments [4].

3.2 Staff Location Tracking

Although the staff location tracking can raise some privacy concerns, it can also give effectual information on the workflow process at both individual level and in center wide operations [4]. Studying people processes and effectiveness might lead to process improvements. The response to external or emergency event can also be monitored to identify the holes and bottlenecks in the process and correlate them to a specific event or/and time. This information can then be used in case studies for further improvement and enhancement plans.

Moreover, staff tracking can be beneficial in medical procedures monitoring and safety regulations enforcement, it can help medical staff to follow certain procedures and steps while performing certain medical task or dealing with a specific case or infection. Wang *et. al* [3] presented a case study that demonstrated the usage of RFID into the medical world. The project was conducted at one Taiwan hospital and aimed at containing Severe Acute Respiratory Syndrome (SARS), a dangerous disease that struck Taiwan in 2003. Part of the project was to monitor the medical staff and the process of dealing with SARS-infection cases.

3.3 Patients Location Tracking

Wearable RFID tags can be used to accurately monitor patient location. Rather than waiting for an unreachable patient, knowing patient's location and availability can help in an effective scheduling of limited resources to keep them more active. RFID can also be used to address safety concerns. For example, by tagging pediatric patients, they can be monitored automatically. Children and newborn security can also benefit from RFID tagging, where a child's location can be easily identified. In some cases, other actions can also be triggered like sounding alarms, locking doors or elevators, or even paging a nurse or guard if a child patient or newborn is moving away[4].

3.4 Theft Protection

RFID can be used to prevent theft and unauthorized removal of equipments by triggering alarms at exists when RFID tagged equipment leaves its intended location. Access control can also be integrated with alarm system to lock/unlock doors and control access to specific spaces.

RFID can be deployed in many other applications in healthcare sector. Some of which require integration into other information systems that go further than the traditional location tracking services. The Patient Safety Validation System is one of these applications which may need tagging patients with RFID tags to uniquely identify patients and tagging things linked to patients such as medical equipment or medication to ensure that the right patient receives the intended treatment or medication in the right dosage at the right time.

Similarly by tagging the new born infants, facility lock-down can be triggered after unauthorized removal of an infant from a secured area [4].

4. RFID and Privacy in Healthcare Sector

RFID technology implementations in healthcare sector require tags to contain unique identifiers that can be linked to uniquely identified individuals and their personal health information. Therefore privacy concern becomes an issue when RFID system is implemented without the proper security and integrity mechanisms. Moreover, radio waves are capable to penetrate through walls, plastic, fabric, and other materials which make it vulnerable to be read out of the line-of-sight and potentially without the consent or even the knowledge of the tagged individual, nevertheless lacking proper traces and evidence that they are being read.

In healthcare environment personal health information, which is usually embedded into the tag, is among the most sensitive part of information, which requires strong justifications for its collection, ongoing use, retention and disclosure. The sensitivity of the data require strong security mechanisms in place to ensure protection against unauthorized access, disclosure, copying, use or modification loss, and theft. Appropriate security safeguards must be applied around retention, transfer and disposal of this information to provide necessary protection [5, 6].

In a recent report released by the privacy commissioner of Ontario [14], the deployment of RFID technology in health sector was classified into three broad categories based on their privacy concerns. Each of these categories is explained below.

4.1Tagging Things

All RFID information systems have automatic identification as the base for these applications. RFID technology has been used as ideal solution for identifying, tracking and locating items because they enhance the visibility and accuracy of tagged items over other technologies like bar codes and other labeling techniques. The result of using this technology could be higher efficiency and effectiveness in automating assets management, locating misplaced items, inventory control, products tracking and tracing as they move through their life-cycle, verification of shipments and product authentication. The key reason of using this technology for this kind of applications is often to improve efficiency.

The uniquely identified data stored on RFID tag refers to things, similar to the usage of product serial number; it is used to uniquely identify items. Usually the collection or use of personally identifiable information is not involved in the processes of tracking and identifying tagged objects and items. Therefore there are no privacy implications or concerns in this type of applications.

4.2 Tagging Things Linked to People

This class of RFID technology deployment requires tagging things related or linked to people. This association can lead to identifiable individuals where their personal information may also be involved. Examples of these items include:

- Medical equipments being used by individuals like patients, staff, or visitors.
- Patient's prescription vials, blood samples or specimens.
- Patient's files and dossiers.
- Access cards assigned to individuals.
- Assets and devices assigned to staff.

As in tagging things, the main purpose of the tagging in this type of applications is to identify and track things that are or may be associated to individuals, therefore privacy become important. The sensitivity of data along with the ease and strength of linkage will determine the magnitude of privacy engagement. In inventory control and supply management, when tracking extends to individuals, their privacy can be impacted, especially when the tagged item travels with that individual.

Unauthorized identification, tracking, monitoring and surveillance are very serious privacy issues especially when the informed consent of the person with tagged objects is lacking. Apparently threats and risks can be even more in case of access cards; as it may extend to identity theft that can be achieved by cloning or hacking the embedded RFID-tag, enabling unauthorized access to sensitive and secure areas [5].

4.3 Tagging People

This class of RFID usage requires tagging to identify individuals deliberately, rather than other items of assets that they may be associated with that individual. When tagging people, the practice is always to focus on the permanence and strength of the link between the individual's tag and his personal information. The following are examples of RFID used to identify and track individuals in healthcare environment:

- Staff identification cards.
- Patient healthcare identification cards,
- Wrist and ankle identification bracelets.
- Implanted RFID chips.

When tagging people, the direct and automatic identification of individuals without even their knowledge or any indication allows this class of RFID deployment to have the greatest risks and threats on personal information among all other classes. These risks and threats are valid and could be raised during both processing and retention of this information. It involves many privacy risks and fears including:

- Covert identification, tracking and surveillance of individuals conducted by other by parties without their knowledge or consent.
- Disclosure and unauthorized revelation of private information.
- Identity theft as a result of RFID identification cloning.
- The construction of profiles and histories about individuals and their behavior without their consent or knowledge.

Although tagging individuals may have the greatest implication on patient's privacy, it can also be used to enhance and increase their privacy. This can be achieved by using RFID enabled identification items like wristbands combined with a secure data store to keep patients' confidential and medical information safe and only accessible from the centralized system rather than printing it in a readable format on the band itself. Additionally by utilizing the RFID enabled identification the risk of misidentifying patients and treatment errors will dramatically be reduced.

5. Personal Privacy Threats in RFID

Privacy threats and issues arise when RFID tagging leads to collection or connection of information about individuals. In this section we will present a survey of the main privacy and security threats posed by RFID technology in general. These threats are a result of the technical properties and attributes of RFID technology and its implementation methodology. In the following two sections, we present some proposed solution and legislations addressing privacy threats and concerns in RFID technology. In [8], Garfinkel *et. al.*identified some of the risks and threats to personal privacy caused by RFID technology.

5.1 Location Threat

Most if not all RFID implementations requires placing covert readers in some locations. These readers create two types of threats. First, monitoring and tracking tagged individuals, therefore their location could be revealed. Second, regardless of who is carrying or using the tagged object, its location is vulnerable to unauthorized disclosure.

5.2 Preference Threat

RFID tag contains a unique identifier in order to uniquely identify objects. It identifies many attributes like the manufacturer, the product type, and the unique identity of the object. Extracting this information can expose customers' preferences to competitors at low trivial cost.

5.3 Constellation Threat

This threat involves in the tracking of unidentified individuals. Regardless of whether the identity of the user is associated with a tag or not, consistent tracking of specific tag enables an adversary to correlate information and gradually establish individual's identity and location of the individual [6].

5.4 Action Threat

When a group of tags are moved simultaneously in the workspace, it could trigger a false alert or a direct legitimate action like video surveillance indicating shoplifting or any other monitoring action. This type of actions inferred individual's behavior as a result of fake alert [7].

5.5 Association Threat

This threat is usually due to the association between the uniquely identified item by EPC-tag and the individual who possesses this item. This can be involuntary and covert association type. Tracking the tagged item will therefore lead to tracking that individual associated with it.

5.6 Transaction Threat

In this type of threats, the adversary can derive information by inferring transmission between individuals associated with RFID constellations. This can be accomplished when tagged individuals move from one environment to another, where the collected information can then be analyzed to construct private information like who met who or what a specific individual was doing during a certain period of time.

6. Privacy Protection - Proposed Solutions

The wide use and spread of RFID technology in many fields raises more and more security and privacy threats, which as a result, several solutions have been proposed, some of which has already been implemented to address these ongoing risks by modify the technology in order to balance the demand for more security with minimal user training or regulatory enforcement.

The main objective of security protocols in an RFID environment is to protect privacy. This can be achieved by addressing both authentication and confidentiality requirements. Authentication is needed to verify the eligibility of the reader to read the data on the tag, while encryption will ensure the confidentiality of the data. In fact, traditional cryptographic solutions cannot be satisfied in the RFID environment specifically in passive tags due their low computational power and limited available space; thus, different lightweight protocols have been developed to satisfy the security needs for RFID environment.

This section enumerates various proposed solutions to address the emerging needs for secure RFID solutions to protect the personal privacy of users.

6.1 Tag killing and Sleeping

User privacy has been addressed by EPC tags with kill command to deactivate the tag permanently [8]. EPC tags are usually included in consumer products; consequently, active tags allow consumers tracking without even their knowledge or consent, besides this activity might not be accepted by those consumers; as it is considered as a threat to their privacy. Therefore, this threat can be eliminated by killing or deactivating the tags at the time of purchase. The main problem with killing is that, the post-sale benefits such as returns, repairs. In addition, some appliances and devices which rely on the embedded RFID-chips, such as smart appliances will malfunction with deactivated tags. Further, some applications require RFID tags not to be killed, instead; they should survive over the lifetime of the tagged-item like in rental products.

Sleeping tag is another solution intended to protect the privacy impacts of using RFID tags. Similar to tag killing the sleeping tag can be deactivated where it still has the ability to be reactivated again. Sleeping tag would still have privacy protection in question especially when any reader could reactivate it again. In addition to privacy concerns, practically, sleeping would be difficult to control and manage.

6.2 Tag Password

In password tag, the tag authenticates the reader before emitting any important information until it received the correct password or PIN code. Although the EPC tag has enough resources to hold and verify passwords or PINs, the dilemma in this solution is that the reader will not be authorized by transmitting the correct tag's password unless it knows the identity of that tag [8].

6.3 Tag Pseudonyms

Instead of using passwords, RFID tag could have a small set of pseudonyms and have it cycle through them whenever it is read. Authorized readers would have the list of all valid pseudonyms to identify the tag upon query. Unauthorized tag tracking on the other hand would be more difficult hence adversaries wouldn't have the correlation of two or more pseudonyms belong to the same RFID-tag [8].

6.4 Blocking

Taking a different approach to enhance privacy, blocking does not involve any alteration to consumer tags. Instead, the blocker RFID tag is configured to prevent unauthorized scanning of tags, while permitting authorized readers to operate normally. Blocking RFID tags relies on an updateable bit named as privacy bit. A tag with privacy bit of '0' enables the public scanning of that tag, where privacy bit of '1' marks the tag as private. This scheme is based on the incorporation of the privacy bit into blocking tags; it defines a privacy zone as a space of identifiers with leading bit of "1" where unauthorized scanning of tags mapped into the privacy zone is prevented.

6.5 Lightweight Cryptographic Primitives

The lightweight cryptographic primitives' main objective is to provide mathematical operations that are simple enough to be translated into digital circuit design, while the complexity is moved into the reader and the backend where a bulk of computations can easily take place in acceptable timely fashion. The following are two lightweight primitives protocols used to maintain privacy in RFID environment:

6.5.1 Minimalist Cryptography

Minimalist is a mutual authentication protocol for RFID system using the traditional challenge-response mechanism. Each tag has its unique identification ID that is provided by the manufacturer. The tag's unique ID is used to create access password on the backend database. The same password is then saved in both the database and the tag. This places the access password calculation on the backend. In addition passive tags in general can generate 16-Bit Cyclic Redundancy Code (CRC) checksum for error detection and 16-bit Pseudo-Random Number Generator (PRNG). These simple tag's features are used to create a challenge-response mutual authentication protocol in every authentication phase. The tag performs encryption using the 16-Bit CRC and the random numbers [9]. This protocol provides security protection against spoofing, replay, tracking, and DoS attacks.

6.5.2 Ultra Wide Band Modulation (UWB)

Using UWB is not a traditional cryptographically way for authentication. This protocol has a high data-rate, low average radiated power that can provide large instantaneous bandwidth; this requires a specifically designed tag to meet the protocol features. UWB protocol uses time division of 65,536 slots, the reader and the tag can have mutual agreement on the time slots to be used for communication. Therefore, it is very difficult for an attacker to guess which time slot is being used. The sender

uses Pulse Position Modulator (PPM) to transmit the data, and the time hopping codes are determined by a Cryptographically Secure Pseudo Random Generator (CS PRGN). The main drawback of the protocol is the requirement of UWB-RFID tags and its feasibility to only low rate data applications. [11]

6.6 Lightweight Cryptography Protocols

The main objective of lightweight cryptographic protocols is to provide robust and secure protocols that are necessary for the lightweight primitives, and where heavy weight primitives are not viable choice. They are established with low computational operating cost and minimal digital logic; they do introduce some delay, but they use minimum amount of resources to encrypt the data communicated between the tag and the back-end database and provide security protection against some known attacks. The following are some examples of such protocols:

6.6.1 Gossamer Protocol

Gossamer protocol [12] is an ultra-lightweight protocol designed for limited RFID resources. Unlike the protocols that are based only on triangular functions (T-functions), the strength of the protocol is in the two functions used ROTbits (Left Rotation of the bits) and MIXbits (Mixing bits). Those two functions are non-triangular and offer the fusion and diffusion functions. The protocol is low-cost and provides better security than the T-functions based protocols.

The protocol comprises three stages: tag identification stage, mutual authentication stage between the reader and tag, and the last stage where the tag and the reader update the new secret key values. Bilal *et. al.*[12] proved that the Gossamer protocol is vulnerable to replay attacks that causes de-synchronization between the reader and the tag (which might result in Denial of Service (DOS) attack). The authors proposed an enhancement protocol to avoid de-synchronization attacks.

6.6.2 Noisy Tag Protocols

The Noisy Tag Protocol [10] protocol is designed to take advantage of the noise that is natural in RF communication, the key sharing occur while a known noise is generated which is known to the legitimate reader. The noise pattern is then eliminated to recover the actual tag response. This creates a communication that is not understood by the eavesdropper as the illegitimate reader cannot recognize the difference between the noise and the real data.

6.6.3 One-Time Codes

Using one-time codes combined with simple operation like the XOR function provided three paths to develop lightweight protocols. Those paths are based on secret key sharing between the back-end database and the tag with the following features:

- Random one-time codes are stored on the tag to be used during the set-up stage.
- The tag one-time shared secrets keys are updated in a secure environment against eavesdropping.
- Otherwise the tag uses a low cost computational method for self-updating manner.

To protect against tag tracing, Ghosal *et al.* [10] presented a mutual authentication scheme between the tag and the reader based on XOR-padding and random tag identifier.

6.6.4 Symmetric Key Encryption

Symmetric key encryption [10] is based on a shared key between the communicating entities; the key length has major effect on the security level, specifically for the time it takes to run brute force attack against it. However, the key length represents a complexity that cannot be handled by an RFID tag, it is infeasible to implement traditional symmetric 128-bit key length cryptography.

For instance The Tiny Encryption Algorithm (TEA) is based on the Advanced Encryption Standard (AES) – 128 bit. The word Tiny comes from the very small code required to run the algorithm. The algorithm is feasible to be used with RFID tags. Although, the algorithm still has some weakness, with some implementation, it is a strong candidate for RFID encryption engine.

6.6.5 Asymmetric Key Encryption

The asymmetric key encryption algorithm is based on key-pairs, a public-key used by the sender for encryption, and a private key by the receiver for decryption. So the public key needs to be shared while the private key is kept secret.

There has been different asymmetric protocols proposed for RFID implementations, the main idea is put the burden of encryption

on the reader and the backend. The tag requires some storage and minimal computation that is feasible to implement on RFID tags.

The server needs to keep a separate key for each tag to preserve the overall security. This will maintain the overall security if a tag is comprised by an attack, the system security remain secure. The objective of the protocol proposed in [13] is to use a single key that can be stored on the device, rather than using multiple keys for different tags that can consume a lot of backend resources by querying every tag ID for its key. This key needs to decode different tag IDs provided that the scheme guarantees security even thought the key is a asymmetric (public-key).

The proposed protocol works by encrypting the tag ID with the server public-key. The server uses the private key to decrypt the ID, the tag has the encrypted ID and it is only decrypted at the server, consequently preserving the ID from attackers. This way the protocol avoids the need the continuous querying of the database or the requirement for tag-reader synchronization.

7. Conclusion

RFID technology has been used widely in many commercial applications over the last few years. Health care sector has a large number of potential applications to adapt this technology as a solution to enhance many of the existing processes to not only benefit from reduction in cost and effort but also to enhance the quality of service and the precision of identification. However, the main obstacle that keeps this technology a step behind is the additional privacy implications as a reason of the reader's mobility and the limited computational power of RFID tags. Although there are a number of proposals for privacy protection, but their effectiveness has not been verified yet. This paper is our preliminary work on identifying these solutions in order to fully study their effectiveness.

References

[1] Amin Rida., Li Yang., Manos Tentzeris. (2010). RFID-Enabled Sensor Design and Application, Artech House©, ISBN-13: 978-1-607083-981-1.

[2] Yan Zhang., Yang Laurence, T., Jiming Chen (eds). (2010). RFID and Sensor Networks: Architectures, Protocols, Security and Integrations, Auerbach Publications.

[3] Shang-Wei Wang., Wun-Hwa Chen., Chorng-Shyong Ong., Li Liu., Yun-Wen Chuang. (2006). RFID applications in hospitals: a case study on a demonstration RFID project in a Taiwan hospital, *In*: Proceedings of the 39th Hawaii International Conference on System Sciences.

[4] Booth, P., Frisch, P. H., Miodownik, S. (2006). Application of RFID in an Integrated Healthcare Environment, Proceedings of the 28th IEEE EMBS Annual International Conference New York City, USA, Aug 30-Sept 3.

[5] Ann Cavoukian, Ph.D., HP Canada. (2008). RFID and Privacy Guidance for Health-Care Providers.

[6] Hyangjin Lee., Jeeyeon Kim. (2006). Privacy threats and issues in mobile RFID, Korea Information Security Agency.

[7] Koien Geir, K. (2007). RFID and Privacy, Telektronikk 2, ISSN 0085-7130, Telenor ASA.

[8] Garfinkel, S., Juels, A., Pappu, R. (2005). RFID Privacy:An Overview of Problems and Proposed Solution. IEEE Security and Privacy.

[9] Cai Qingling., Zhan Yiju.,Wang Yonghua. (2008). A Minimalist Mutual Authentication Protocol for RFID System & BAN Logic Analysis, Computing, Communication, Control, and Management.

[10] Sayed Ahson and Mohammad Ilyas. (2008). RFID Handbook: applications, technology, security and privacy, CRC Press, ISBN: 978-1-4200-5499-6.

[11] Dong Sam Ha., Patrick R. Schaumont. (2007). Replacing Cryptography with Ultra Wideband (UWB) Modulation in Secure RFID, IEEE International Conference on RFID.

[12] Zeeshan Bilal., Ashraf Masood., Firdous Kausar. (2009). Security Analysis of Ultra-lightweight Cryptographic Protocol for Low-cost RFID Tags: Gossamer Protocol, International Conference on Network-Based Information Systems.

[13] Yang Cui., Kazukuni Kobara., Kanta Matsuura., Hideki Imai. (2007). Lightweight Asymmetric Privacy-Preserving Authentication Protocols Secure against Active Attack, IEEE International Conference on Pervasive Computing and Communications.

[14] Ann Cavoukian., Victor Garcia. RFID and Privacy: Guidance for Health-Care Provider, Available Online at http://www.ipc.on.ca/images/Resources/up-1rfid_HealthCare.pdf