Chapter 21
Data Privacy Issues with RFID in Healthcare

Peter J. Hawrylak and John Hale

Abstract Radio frequency identification (RFID) provides a means to implement the "last-mile" connection in a connected world, often referred to as the Internet of Things (IoT). RFID has been widely used in the retail and construction sectors for supply-chain management, and has provided significant benefits to those sectors. RFID has also been employed by healthcare to improve supply-chain management and monitor the locations of patients and providers to improve service offerings. The wireless and low-cost aspects of RFID introduce privacy concerns. However, there are some privacy issues related to the use of RFID, including tracking and the ability of an attacker to obtain sensitive data that is stored in the RFID tag. This chapter will explore the use of RFID in healthcare and identify issues relating to privacy that need to be addressed in these use-cases. An overview of RFID technology is presented followed by an overview of applications of RFID in healthcare. The privacy issues are then identified and potential solutions described. The privacy issues identified can be addressed using proven and standard security practices, many of which are already implemented by healthcare providers. A discussion of how to extend these practices to include RFID technology is provided.

21.1 Introduction

Radio frequency identification (RFID) is a key component of the connected world and the Internet of Things (IoT). There are many applications of RFID in medicine, from managing inventory to monitoring patient's health. The wireless nature of RFID coupled with the requirement for a low unit price of RFID tags introduces several privacy concerns. This chapter provides a brief overview of the use-cases of RFID in medicine and then provides a thorough analysis of the privacy issues and risks associated with these systems. Solutions to these risks are hypothesized and the impact of the proposed solution is estimated on the original use-case.

P.J. Hawrylak (✉) • J. Hale
Tandy School of Computer Science, The University of Tulsa, Tulsa, Ok, USA
e-mail: peter-hawrylak@utulsa.edu; john-hale@utulsa.edu

A. Gkoulalas-Divanis, G. Loukides (eds.), *Medical Data Privacy Handbook*,
DOI 10.1007/978-3-319-23633-9_21

21.1.1 RFID as a Technology

RFID is a form of wireless technology, which has wide adoption in supply chain management (inventory tracking), and will play a key role in the development and deployment of the Internet of Things (IoT). RFID provides the *last-mile* connection between the asset or object and the larger information system, i.e., the Internet. RFID systems consist of two basic components, the RFID tag, which is attached to assets, and the RFID reader, which provides the gateway between the tags and the larger information system (Internet).

RFID tags contain a unique identifier (UID) that is used to identify a single RFID tag out of a group of RFID tags. This is in contrast to a barcode system where the barcode represents the serial number of the item, but is not unique; the quantity of items is determined by the manual process of scanning the barcode on each item. The UID of the RFID tag can also double as an address, or IP address, for the tag and item it is associated with. In this manner RFID provides a way to assign IP addresses to objects to create the IoT. RFID tags that provide only their UID are referred to as "license plate" RFID tags as they just provide a license plate for an item but no additional information.

A RFID tag can provide higher functionality beyond the license plate tag, by including additional re-writable memory or sensors in the tag. These tags are sometimes referred to as "data-rich tags." The additional memory can be used to store information such as product expiration dates or to provide a record of maintenance activities on an item.

RFID tags generally fall into one of three categories, passive, battery assisted passive (BAP), and active, based on how they are powered. Passive tags do not have an on-board power source and must harvest their operating energy from their ambient surroundings. Often, they harvest energy from the radio frequency (RF) signal from the RFID reader. Passive tags communicate using backscatter communication, which is low-power and does not require the tag to contain a transmitter. Tag cost and operating energy requirements are the major limiting factors in functionality provided by passive tags.

BAP tags are positioned between passive and active RFID tags in terms of functionality and cost. BAP tags include a on-board power source (e.g., a battery) for non-communication operations, such as sensing between reads. Communication is accomplished using backscatter. The inclusion of the power source allows the BAP tag to use all of the RF energy from the reader transmission for backscatter resulting in a longer read (communication) range compared to a passive tag. BAP tags are widely used applications that require sensing or monitoring because they can take readings between reads. Passive tags are only powered during the read and that is the only time they can take a reading.

Active tags are typically the most costly, have an on-board power source, and use an active (powered) transmitter and receiver. They support long-range communication and can communicate in areas unfriendly to RF communication (e.g., significant RF noise). Communication ranges vary based on the type of transceiver and battery in the tag. Typical ranges for active tags in RFID and RTLS applications range from tens of meters to several kilometers. Active tags are widely used to monitor conditions, such as intrusion detection in shipping containers, and transmit alerts of abnormal conditions (e.g., over a satellite link). In addition, active tags are often used to track objects and people in a real-time location system (RTLS). The active transmitter and receiver support advanced location determination algorithms to be executed to determine the precise location of the tag.

There are several RFID communication protocols that are used in RFID systems. Differences between these protocols include the frequency bands used, data formatting, data encoding, and supported commands. All protocols provide a means to obtain the UID from the RFID tag, but several include support for reading and writing small user-memories on the RFID tag. These user memories are between 100-bits to several mega-bits (Mb).

From a frequency band perspective RFID systems operate in four different bands: 125–135 kHz, 13.56 MHz, 433 MHz, and 860–960 MHz. The 125–135 kHz band supports low-frequency (LF) RFID systems. These systems are typically passive and operate in the near-field. They are used for livestock and animal tracking because to the ability of the LF signals to penetrate animal tissue. The read-range (distance between the reader and tag, when the tag can be successfully read) is about 30 cm.

The 13.56 MHz band supports high-frequency (HF) RFID systems. These systems are passive RFID systems and operate in the near-field. HF RFID is used in many access control systems (badge systems), contactless payment, public transit fare collection, and supply chain management. The 13.56 MHz band is designated as an industrial, scientific and medical (ISM) band worldwide, which means that it can be used without a license anywhere in the world. This makes HF RFID a good choice for implementing systems that need to work around the world. HF RFID provides better read ability when tags are in the presence of liquid and HF RFID has been identified as one option for using RFID to meet ePedigree mandates for pharmaceuticals. HF antennas are typically designed using a loop structure and some examples of HF tags are shown in Fig. 21.1.

The 433 MHz band supports ultra-high frequency (UHF) active RFID systems. These systems are used to track large assets such as shipping containers and have a read-range of up to several hundred meters. They can communicate with the reader in environments that are not friendly to radio frequency (RF) communication (e.g., large amounts of metal such as on a cargo ship).

The 860–960 MHz band supports UHF passive RFID systems. These systems are used in supply-chain management and inventory tracking applications. There is no frequency band in this range that is available worldwide. Thus, each country uses a different frequency band in this introduces problems in the design of the antenna for the RFID tag. Specifically, it is difficult to design an antenna that will work well over the entire 100 MHz band and still meet the low price point and small area requirements for RFID tags. Often, the size of the object being tagged limits the size of the RFID tag. The EPCglobal organization manages the Electronic Product Code (EPC) numbering system that manages the tag UIDs used by different users.

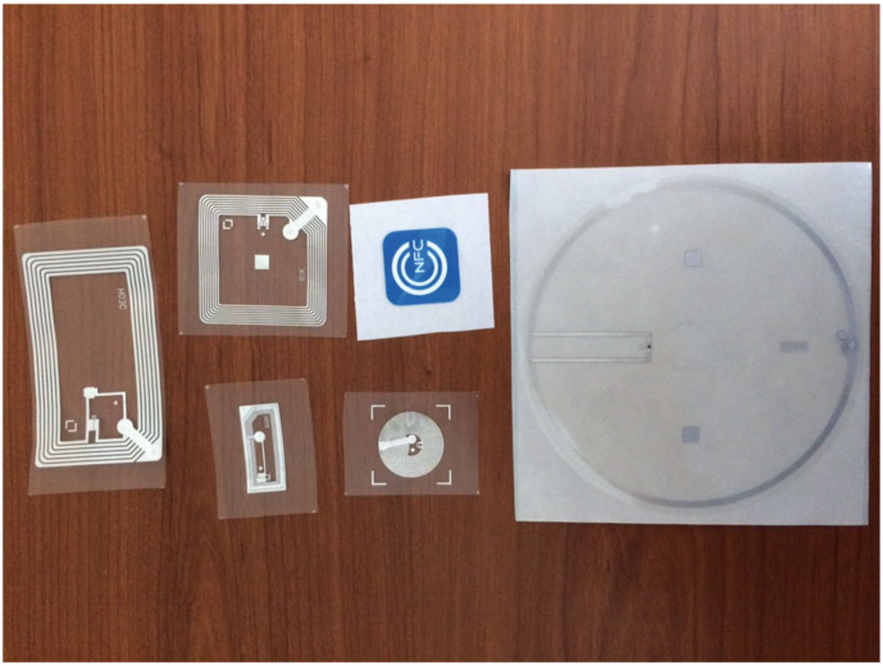

Fig. 21.1 Passive HF RFID tags

The EPC number is used as a key to lookup the item in a central database where detailed information about that item is stored. Thus, it is important that each user assigns UIDs from within a set of numbers that are assigned to them. This is similar to how IP addresses are allocated and managed. UHF antennas are typically based on a dipole instead of a loop. Examples of UHF tags are shown in Fig. 21.2.

The UHF passive RFID systems also support the inclusion of batteries to create a BAP RFID system. The typical application of a UHF BAP RFID system is to attach sensors to the RFID tag to monitor conditions between read events. Table 21.1 shows frequency band, corresponding RFID system type, the applicable ISO standards, and typical applications of these systems.

The remainder of this chapter is structured as follows. Section 21.2 presents the privacy needs for medical data and provides a high-level framework for accessing privacy concerns and to define when a breach occurs. Next, Sect. 21.3 presents applications of RFID in medicine, with a focus on applications for inventory tracking, tracking people, and device management. The use of RFID in each area are presented along with example applications. Then, Sect. 21.4 describes the risks to privacy associated with these three use-cases for RFID in medicine. Section 21.5 presents some potential solutions to these issues. Finally, Sect. 21.6 concludes this chapter by summarizing the issues and solutions that were presented.

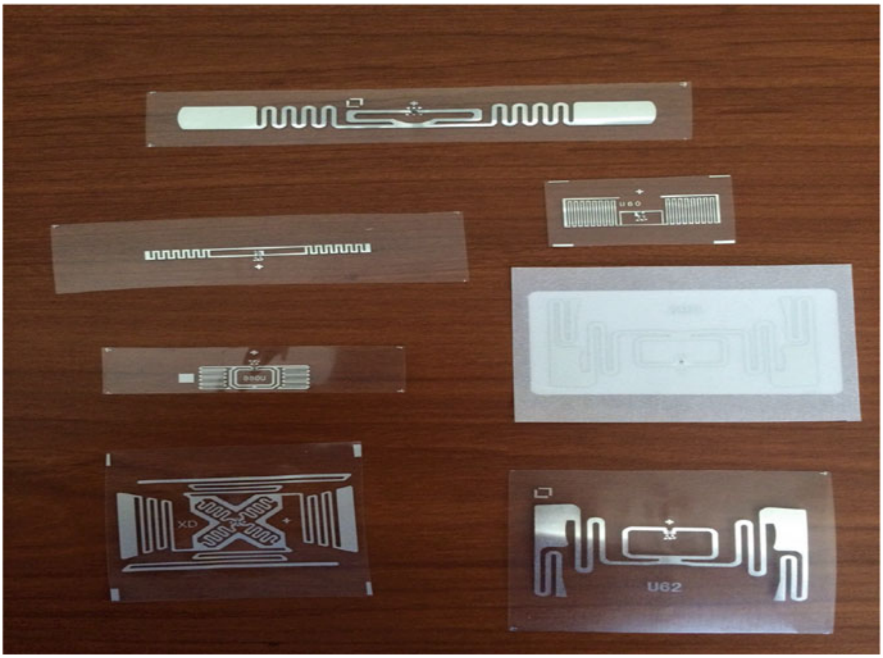

Fig. 21.2 Passive UHF RFID tags

Table 21.1 The frequency band, RFID type, corresponding ISO standard, and typical applications

Frequency band	RFID type	ISO standard	Typical application
125 kHz	LF	ISO 18000-2	• Livestock and pet tracking
13.5 MHz	HF	ISO 18000-3	• Public transit fare • Access control systems
433 MHz	UHF (active)	ISO 18000-7	• Tracking shipping containers
860–960 MHz	UHF (passive)	ISO 18000-6 (air interface) • ISO 18000-61 (Type A) • ISO 18000-62 (Type B) • ISO 18000-63 (Type C) • ISO 18000-64 (Type D)	• Supply chain management

21.2 Dimensions of Privacy in Medicine

Privacy in the modern age is commonly concerned with controlling the disclosure of identifiable information. Today, medical data is often digitized and transmitted between information technology (IT) systems to facilitate diagnosis, treatment and care. Much of that data is often considered to be protected health information (PHI), as it contains sensitive and identifying information. PHI includes items such as data of birth, home address, contact information (e.g. home address, telephone numbers, and email address), emergency contacts, treatment details, and medical history.

The foundations of medical privacy rest in principles promoted by the 1973 HEW Report, a study conducted by The Secretary's Advisory Committee on Automated Personal Data Systems within the Department of Health, Education, and Welfare [1]. The study [1] established a Code of Fair Information Practices comprising five ideals:

1. There must be no personal-data record-keeping systems whose very existence is secret.
2. There must be a way for an individual, to find out what information about him is in a record and how it is used.
3. There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent.
4. There must be a way for an individual to correct or amend a record of identifiable information about him.
5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data [1].

The Code of Fair Information Practices profoundly shaped the Privacy Rule in The Health Insurance Portability and Accountability Act (HIPAA) of 1996. HIPAA was passed by the U.S. Congress with five objectives: improving portability and continuity of health insurance coverage; combating waste, healthcare fraud, and abuse; promoting medical savings accounts; improving access to long-term care services; and simplifying health insurance administration [2, 3]. HIPAA's Privacy Rule establishes conditions to preserve patient privacy in healthcare systems. Other aspects of HIPAA deal with privacy indirectly by incorporating provisions intended to preserve security properties of patient data in any form.

Concerning privacy, HIPAA prescribes how an individual's PHI can be collected, used, or disclosed. Identifying information such as billing records, data entered by healthcare providers, patient information stored in the computer system, and the health insurer's information about treatment and care, are protected by HIPAA. The Privacy Rule permits access to PHI only when providing treatment, paying medical providers for services, protecting public health, giving reports to law enforcement, or when a patient has explicitly authorized a third party. HIPAA applies to any organization that touches PHI. This includes healthcare providers, health plan providers, and business associates.

The 2009 Health Information Technology for Economic and Clinical Health (HITECH) Act gave the U.S. Department of Health and Human Services (HHS) the authority to create programs for private and secure electronic health information exchange [4]. The Omnibus Rule by the Office for Civil Rights clarified and expanded the scope of HITECH's and HIPAA's privacy and security provisions. This rule increases the liability of business associates, broadens the right of individuals to PHI access and notice, and increases privacy protection for genetic information [5].

The Office of the National Coordinator (ONC) in HHS has adopted eight privacy principles essential for privacy solutions in healthcare information systems [6]:

1. **Individual Access:** Simple and timely access for individuals to their personal health information.
2. **Correction:** Ability of an individual to dispute and correct erroneous personal health information.
3. **Openness and Transparency:** Openness and transparency of policies, procedures and practices relating to an individual's medical records.
4. **Individual Choice:** Ability of an individual to make informed decisions regarding the collection, use and disclosure of their personal health information.
5. **Collection, Use and Disclosure Limitation:** Appropriate control of the collection, use and disclosure of personal health information governed by the necessity to accomplish a specific purpose.
6. **Data Quality and Integrity:** Reasonable effort to guarantee personal health information has not been altered inappropriately and that information is accurate.
7. **Safeguards:** Application of security controls to preserve the confidentiality, integrity and availability of medical records and personal health information.
8. **Accountability:** Monitoring and reporting of events and actions in HIEs that potentially constitute breaches, misuses or violations of privacy and security.

The wireless nature of RFID introduces and magnifies several privacy concerns. Specifically, the wireless communication link provides the attacker the ability to launch an attack from a distance. An example of such an attack is using a rogue RFID reader to retrieve (read) the data from an RFID tag that contains medical data about a patient, in order to obtain that patient's PHI. Solutions to address this concern and other potential attacks are presented later in this chapter. Further, the low-cost and low-power (especially for passive tags) requirements for the RFID tags limit the available security and privacy measures that can be implemented. However, most of these concerns can be addressed using typical techniques.

A recent analysis of security concerns for RFID tags [7] of Gen-2 and ISO 18000-63 [8] passive ultra-high frequency (UHF) tags identified four major categories of attacks: interception, interruption, modification, and fabrication. Of these interception is a direct threat to privacy because personal information could be obtained from the transmission or the intercepts used to track a person. Tracking can be used to extract further personal information about the person by linking the rooms of the medical facility they visit to the services provided by those rooms (e.g., cancer treatment). One application is to reduce waiting times [9] by keeping track of the location of patients and providers.

21.3 RFID in Medicine

RFID and RTLS offer many benefits to medicine and have been successfully applied to address several issues. A general overview of these technologies can be found in the following: for RFID [10–14], and for RTLS [15–17].

This chapter focuses on the following use-cases of RFID and RTLS technology in medicine: (a) *inventory tracking*, (b) *tracking people*, and (c) *medical device management*. These use-cases are described in further detail in the following sections.

21.3.1 Inventory Tracking

Inventory tracking and supply chain management is a major use-case for RFID, especially in the retail sector [18]. Tracking inventory and linking the use of supplies to the appropriate patient is a major issue for most hospitals. RFID has been used to create "smart cabinets" that are able to link supplies that are removed to a particular patient [11]. This enables better billing accuracy and can be linked into hospital inventory management systems to ensure that supplies are reordered when they are needed. Several users have realized savings from a reduction in the number of items that expire before use from such systems [19–21].

Another use of RFID is to monitor whether or not a patient is taking their prescribed medications. One implementation uses a specially designed drawer with a RFID reader and RFID tags on each medicine container to track when a patient removes medicine from the drawer [22]. This system records what medications were removed and replaced, but does not verify the dose of the medication taken (e.g., how many pills were removed). An expansion of this system was implemented to include the ability to record the weight of the medication container before and after removal [23]. Another system incorporates a video camera to track medication for elderly patients to ensure compliance with the prescribed instructions [24]. Another medication compliance system uses a RFID reader contained (at least the antenna) in a necklace with a tag in each pill to monitor when a pill is ingested [25]. General RFID systems integrated into hospitals can be used to help providers maintain supply levels and can potentially allow them to move closer to the just-in-time inventory process used in many retail establishments [26]. Other uses include using RFID systems to track the location and status of digital infusion pumps [27].

21.3.2 Tracking People

RFID and RTLS provide a means to track people in an environment. There are a number of means to determine the location of the RFID tag in an environment, including range estimation based on signal strength [28–32] time-of-arrival/flight [33–36], and angle of arrival [37, 38]. Other more advanced options to get better accuracy are possible.

The medical applications in this area often focus on tracking patients of care-facilities [39] and tracking locations of patients and staff members in a doctor's office for scheduling purposes. Several researchers have also investigated using RFID to locate and track patients and providers for the purpose of improving workflow planning and management [40]. The ability to track patients allows the care facility to monitor the location of at-risk patients (e.g., those suffering from memory loss diseases) and to be alerted if the patient leaves the facility or enters an a restricted or unsafe area. One study looked at the use of a commercial RTLS system to monitor the entry/exit points of a hospital [41]. Alerts are triggered when a patient passes through a entry/exit point. One benefit of monitoring only entrance and exit points is a reduction in the number of RFID readers needed to monitor a facility. This reduces the cost of the system. However, the downside of this is that the patient's location cannot be tracked inside the facility but only at entry/exit points. This is effective for many facilities because they only need to monitor the entrances and exits points and not the entire facility.

Systems have also been deployed using RFID and other Internet of Things type technologies to track how a person interacts with their environment [24, 42, 43]. These systems can be used to help manage patients suffering from cognitive diseases while allowing them to remain in their homes or have more independence compared to a traditional nursing home.

Other systems track the location of patients and can be used to help control the spread of infectious disease. One such system was implemented in a hospital in Taipei to help control the SARS virus [44] by identifying patients with SARS symptoms or diagnosed with SARS, and also by identifying the individuals that were in contact with a person newly diagnosed with SARS. This system helped to isolate those patients with SARS and those medical workers assigned to treat SARS patients from the rest of the hospital's population. Many other RTLS systems have been applied to improve processes in hospitals [9, 45–48].

21.3.3 Device Management

RTLS systems have been used to track and locate devices and equipment within a hospital [41]. These RTLS systems differ from those issuing alerts when people leave a facility without authorization in that they track the location of devices (objects) in the entire facility. One concern with wireless location systems is being able to read through walls in a building. For example, this could result in the system indicating that an asset is in room 314 when it is actually next door in room 315.

RFID provides the ability to track inventory, including medical supplies and pharmaceutical drugs. Inventory tracking using RFID is a common application of the technology in the retail sector. In the retail sector RFID is being used to reduce the time (man-hours) required to take inventory [49, 50] and in some instances can be used to give a merchant an instant view of inventory on hand in their store. This information is then used to ensure that the optimal product selection [51] is available on the store shelves to customers and that something ordered over the Internet is actually available for pickup in the store.

Similar methods can be applied to healthcare to track medical supplies. RFID can be used to link supplies used to a particular patient, to help ensure that each patient is charged for only those supplies that they use. The hospital can use this information to improve the accuracy of their inventory and can reorder needed supplies so that they arrive just-in-time for their use. Another use of RFID is to identify the patient to verify their medications [52]. This helps reduce the occurrence of the medical issues arising from giving patient A, patient B's medications. This application also simplifies the nurse's task in delivering the medications and should result in less time being spent on delivery of the medication, allowing more time for patient interaction and providing care service.

A RFID system was pilot tested in a hospital in Cyprus to identify patients and track inventory in the pharmacy [26]. Identification of patients is a key factor in providing the correct medical treatment and is often the root-cause for medical mistakes. One such application of this technology is to link the patient to their medication to ensure that each patient receives the proper medication and dosage. In the system presented in [26] the pharmacists found benefit in the improved and quick inventory features provided by the system, which helped them to maintain the optimal supply of medication in the pharmacy.

21.4 Issues and Risks

Privacy issues differ from security in that privacy is geared to the collection, use, and release of confidential information. Security is concerned with confidentiality and also data integrity and availability. With respect to privacy, the requirement to have access to the data—availability—is often at odds with the need to maintain confidentiality of the data. For example, a secure system that provides sufficient confidentiality will provide privacy protection. However, in medicine, it is sometimes hard to enforce access control, especially in response to an emergency situation. For these emergency type situations several medical databases allow qualified medical professionals to gain access to a patient's medical information for treatment purposes, even if they do not normally have access rights to that information. Medicine introduces limits on the time required to obtain information (e.g. or risk the patient dying) that in other industries (e.g. financial institutions) are not present and allow for alternative means of authenticating the user or providing a redacted version of the data to the user to allow them to perform their task. The low cost nature of RFID tags makes the inclusion of strong security options difficult. Further, passive RFID devices must harvest enough energy to power the tag during strong, and often long, cryptographic operations. An overview of security and privacy concerns relating to RFID is found in [53].

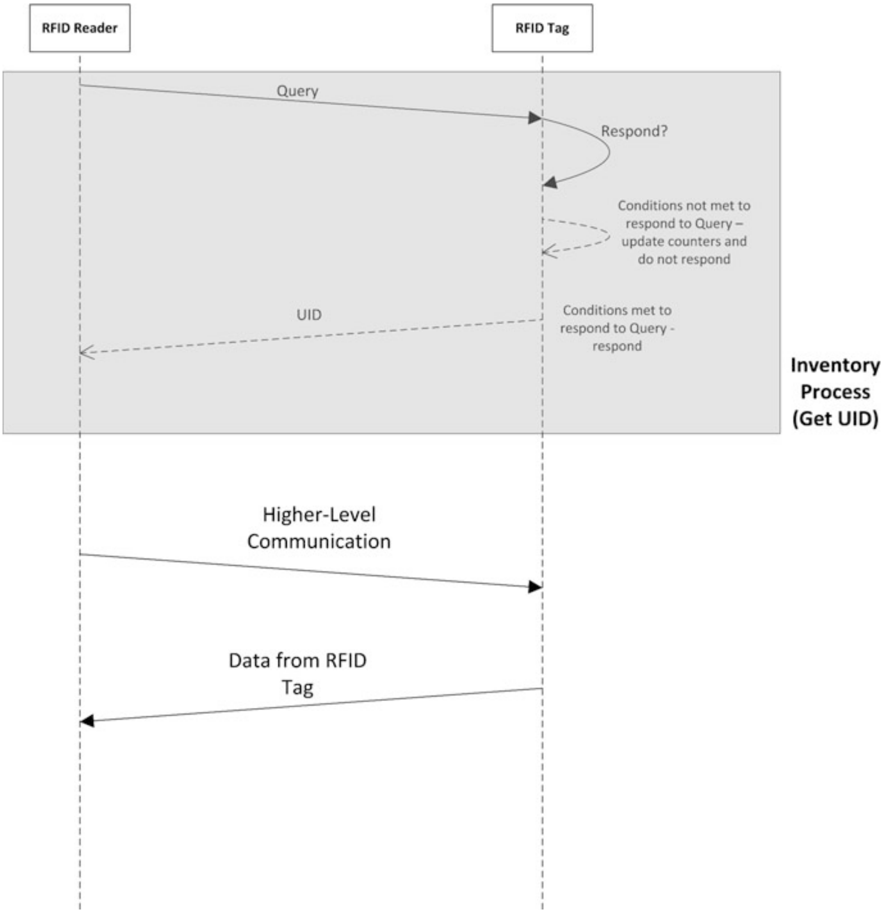
RFID Reader
RFID Tag
Query
Respond?
Conditions not met to respond to Query – update counters and do not respond
UID
Conditions met to respond to Query - respond
Inventory Process (Get UID)
Higher-Level Communication
Data from RFID Tag

Fig. 21.3 Basic exchange between an RFID tag and reader

Tracking is difficult to prevent because the mainstream RFID protocols require each tag to have a unique identifier. A typical RFID exchange begins with the reader retrieving the UID from one tag and then using the UID to carry out a higher-level communication where data (from the user data section) of the tag is read by the reader. Alternatively, the higher-level communication session could be used to set operating or security parameters of the tag, or to write data to the tag's user memory. All tags support the capability to retrieve the UID, but not all support the higher-level functions (or have user memory). Figure 21.3 shows the basic components of the RFID exchange. The first part recovering the UID is supported by all RFID tags, while the second part (higher level communication) is supported by some tags.

There are several proposed solutions to address tracking [54–56], but most require significant infrastructure on the part of the system. This large infrastructure overhead may not be feasible for pervasive systems such as those envisioned in the IoT. The Internet of Things concept requires every device to have a unique address (similar to an IP address) and this means that these devices will be easy to track, which is often beneficial for the Internet of Things applications, but troubling from a privacy standpoint. Ideally, the same RFID tag could be used to provide information and services from the point of manufacture (or assignment) to the point where it is discarded or returned (recycled). This is one of the goals of the EPC numbering system. New additions to the EPC Gen-2 protocol (basis for the ISO 18000-63 standard) include commands to support security features to authenticate readers to tags and to provide communication channels that ensure confidentiality and integrity of the data and higher-level commands passed between the reader and tag [57].

The EPC number provides a unique key to search in a centralized database to obtain additional information about a RFID tag and the item or person it is associated with. This process allows the RFID tag to contain only "license plate" data to link the tag to an entry in the database. Hence, RFID tags providing only a unique ID that can be used as a search key for a database are termed "license plate tags." Figure 21.4 shows this process. Typically, a user-interface is involved to present data to the user and often times offers data entry capabilities to the user. First, the RFID tag is singulated, which means that it is identified by the reader out of the collection of RFID tags present. Once singulated, the RFID reader can retrieve the tag's EPC number and can perform higher-level operations (e.g. read and write user-memory) with the tag. The EPC number is then used by the reader to query the central database. The central database holds detailed information about the tag and associated asset and provides this information to the user-interface. At this point, the user can request additional operations to be performed on the tag or can alter data in the database. This model separates the data storage from the RFID tag and this has benefits from a privacy perspective because strong authentication procedures can be implemented to protect the database and the tag only carries the EPC number (license plate). One drawback of this division of information is that the data may not be available to the user if they do not have a connection to the central database.

A recent survey of RFID applications in healthcare found that privacy was a significant factor in the success or failure of an RFID deployment that involves tracking individuals, but not assets [17]. The concern includes both patients and healthcare providers. While the EPC Gen-2 protocol and ISO 18000-63 standard include support to permanently disable the digital components on a RFID tag, through a kill command, using this feature prevents the RFID tag from being used in the future. Physical means can also be used to achieve similar results by damaging the antenna by including a removable piece in the antenna to reduce the read range to a few centimeters [58].

One of the difficulties is that for hospitals to adopt RFID and RTLS technology the system needs to be able to integrate with the other systems present in the hospital [59]. These systems include data entry and collection systems, central databases, and user interfaces. The data entry and collection systems need to be able to interact with the RFID readers directly or through middleware (e.g., a device

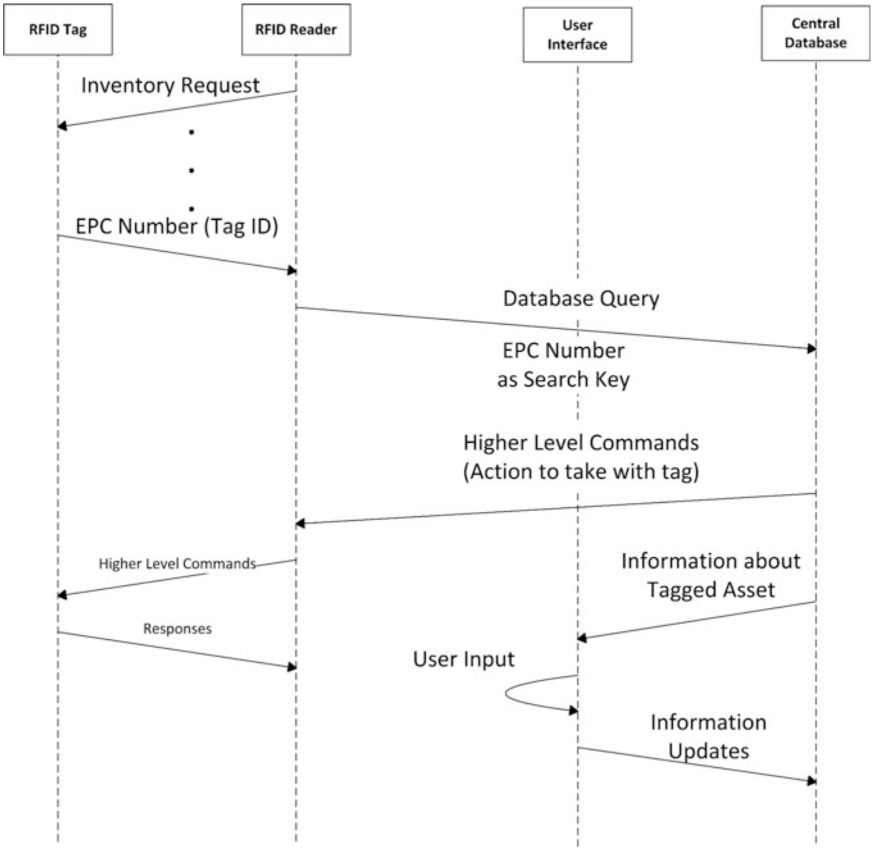

Fig. 21.4 Using the EPC number to retrieve additional information about the tag and associated asset

driver) software to have the readers establish and manage communication between the larger system and the RFID tags. The middleware or the reader can also process the RFID tag data and present it in a format expected by the hospital's larger system. The medical database needs to include additional fields to hold tag UIDs to link those to a particular patient or asset, and must supply space to hold additional data provided by the RFID system. The user interfaces must provide the ability to interact with the RFID components, including input for the data that is stored in each tag and provide a means to select a particular tag (e.g., a list of asset serial numbers or patients). The need to share data among different systems introduces potential privacy concerns. However, these concerns can be addressed by ensuring that all components in the larger system comply with the facility's privacy requirements.

RFID provides a platform to expand this sharing of information and can even be used to store small subsets of a person's medical information. In one system [60] RFID tags are used to store a patient's critical care information in plain-text to allow first-responders to quickly access this information, without having to move the patient, to provide treatment while waiting for their information to be retrieved from their insurance provider. This system is also useful in areas where there is no access to the patient's health provider. However, this system does not address privacy issues well because the data is stored as plain-text allowing anyone to read it, but this feature is needed to provide the access for the first-responders. This example represents one key issue with privacy: how to limit access to the data from unauthorized users, while providing as many authorized users access as possible.

Confidentiality of information is another key concern for users in healthcare. Encryption is one standard means of protecting the confidentiality of information and can be used to protect the data stored in the RFID tag. While RFID tags offer limited support for high-strength cryptology, the encryption could be performed on the reader side and then the encrypted data stored on the tag. Further, higher-strength authentication and encryption methods can be employed by the backend system (e.g., database) to ensure confidentiality and availability of the information. Care must be taken to ensure that an attacker cannot infer information from the encrypted text (e.g., identify which tags have data about a cancer medication). One method of this attack is to use the Select command in the Gen-2 protocol to search user-memory on tags to identify tags with a particular bit pattern [7]. However, this attack can be prevented by using a hash function to help randomize the encrypted text that is stored in the tag for each instance.

21.5 Solutions

Tracking is a difficult problem to address in RFID because of the need to have the tag function with readers spread over a wide geographic area and controlled by a number of different institutions. However, the read ranges of most passive RFID systems are less than 5 m in free space (e.g., an open air environment) so this makes tracking someone exclusively using RFID readers difficult. Physical surveillance would most likely be a better option, because using RFID readers would require a large reader infrastructure and the attacker to have access to all of those readers (e.g., they must hack into each reader). In healthcare, access to a patient's medical history (file) or electronic health record would provide the attacker with more information.

Confidentiality of the data stored in the RFID tag can be protected using encryption. New additions to the Gen-2 specification provide support for stronger encryption of data and for the establishment of confidential communication channels [57]. Further, ISO is developing a family of standards, ISO 29167, to standardize the deployment of security options (called "suites") for RFID systems described in the ISO 18000 series of standards. ISO 29167-1 provides the requirements and basis for identifying the different security options; other parts in the ISO 29167 series (ISO 29167-11 defines the PRESENT-80 security suite) will define implementation of individual security options for RFID. These standards provide a unified blueprint for developers and users to implement security options for RFID systems to meet the requirements for healthcare.

Moving the encryption and decryption operations to the backend systems, the facility's internal authentication system can be employed to prevent unauthorized access to data. The license-plate tag offers some benefits from the privacy standpoint because it contains no information other than the unique search key used during the database query process to obtain the record matching the patient (patient is linked to a unique serial number stored in the RFID tag). An attacker obtaining the tag's ID would still need to obtain access to the facility's system to access the patient's PHI which is stored in the database and not on the tag. If the attack can get into the facility's database (system) they have no need to interact with the RFID side of the system because the database contains the PHI and personal contact information for all of the facility's patients.

21.6 Conclusion

This chapter presented use cases of RFID and IoT technology in healthcare. Privacy issues associated with these technologies specific to the healthcare sector have been identified and potential solutions discussed. Tracking and confidentiality of information were the two privacy threats present in the healthcare environment. Tracking is the most difficult issue to eliminate because most mainstream commercial RFID protocols are based in part on the ability of the reader to retrieve the tag's ID number. While some methods have been proposed to address tracking RFID tags by using pseudo-IDs that change with each read (inventory) these methods require significant infrastructure and result in a closed system. In such a closed system, the RFID tag will only be able to be accessed (read) by readers within that system. This is in contrast to the IoT vision where devices, such as RFID tags, will work seamlessly with any reader to allow the RFID tag to provide maximum value or service to the user. Moving to a connected or IoT world will require systems that can support the authentication of many low-functionality devices efficiently. Physical tracking is probably a better alternative to tracking using RFID readers. Basic physical security practices, such as limited access areas (e.g., not allowing the general public into the exam areas without an escort) can prevent most tracking, either physical tracking or tracking using handheld RFID readers. Security solutions exist to address the other issues associated with RFID systems in medicine. In summary, the ability for patients to opt-out of using the RFID systems should be sufficient, as this will allow those who wise to avail themselves of the benefit to do so, it will also allow those that do not want the risk of tracking via RFID tags to accomplish that too.

The confidentiality of data stored in the RFID tag is of greater concern. The result of unauthorized access to medical data stored in the RFID tag's user-memory is a significant threat to privacy. However, this situation is easy to prevent, through the use of encryption to protect the stored data from unauthorized access. This will prevent the attacker from being able to use of interpret the data in the event that they are able to retrieve it from the tag. Further, the new security features of the EPC Gen-2 specification and new family of ISO standards defining how to implement security and the associated security implementations (ISO 29167 family of standards) harden the RFID tags to resist unauthorized access of their user memory.

In conclusion, RFID and IoT technologies have already been used in healthcare to provide significant savings to providers, improve patient safety (e.g., ensure each patient receives the correct medications), and reduces patient waiting times have been deployed and show proven results. RFID has been used in a number of hospitals to track hand washing compliance which is one of the top ways to prevent the spread of infections. In most cases, compliance levels increased after installation of such a system. The privacy concerns identified in this chapter (tracking and confidentiality of data) can be addressed by standard solutions and procedures already employed by healthcare providers.

References

1. Department of Health, Education and Welfare. Records, Computers and the Rights of Citizens: Report of the Secretarys Advisory Committee on Automated Personal Data Systems (1973)
2. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104–191, 110 Stat. 1936 (1996)
3. Jacques, L.B.. Electronic health records and respect for patient privacy: a prescription for compatibility. Vanderbilt J. Entertain. Technol. Law **13**, 441 (2010)
4. Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 (2009)
5. Federal Register. 45 CFR Parts 160 and 164 Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule (2013)
6. Office of the National Coordinator. Connecting Health and Care for the Nation; A Shared Nationwide Interoperability Roadmap (2014)
7. Hawrylak, P.J., Schimke, N., Hale, J., Papa, M.: Security risks associated with radio frequency identification in medical environments. J. Med. Syst. **36**(6), 3491–3505 (2012)
8. International Organization for Standardization: ISO/IEC DIS 18000-63 Information technology – Radio frequency identification for item management – Part 63: Parameters for air interface communications at 860 MHz to 960 MHz Type C (2013)
9. Sanders, D., Mukhi, S., Laskowski, M., Khan, M., Podaima, B.W., McLeod, R.D.: A network-enabled platform for reducing hospital emergency department waiting times using an RFID proximity location system. In: International Conference on Systems Engineering, pp. 538–543 (2008)
10. Hanada, E., Kudou, T.: Effective use of RFID in medicine. In: 2013 7th International Symposium on Medical Information and Communication Technology (ISMICT), pp. 76–80 (2013)
11. Bendavid, Y., Boeck, H., Philippe, R.: RFID-enabled traceability system for consignment and high value products: a case study in the healthcare sector. J. Med. Syst. **36**(6), 3473–3489 (2012)
12. Mickle, M.H., Mats, L., Hawrylak, P.J.: Physics and geometry of RFID. In: Ahson, S., Ilyas, M. (eds.) RFID Technologies and Applications, Technology, Security, and Privacy, pp. 3–16. CRC Press, Boca Raton (2008)

13. Hawrylak, P.J., Cain, J.T., Mickle, M.H.: RFID tags. In: Yan, L., Zhang, Y., Yang, L.T., Ning, H. (eds.) The Internet of Things: From RFID to Pervasive Networked Systems, pp. 1–32. Auerbach Publications, Boca Raton (2008)
14. Dehaene, W., Gielen, G., Steyaert, M., Danneels, H., Desmedt, V., De Roover, C., Li, Z., Verhelst, M., Van Helleputtea, N., Radioma, S., Walravens, C., Pleysier, L.: RFID, where are they? In: Proceedings of ESSCIRC, 2009, pp. 36–43 (2009)
15. Lee, W.J., Liu, W., Chong, P.H.J., Tay, B.L.W., Leong, W.Y.: Design of applications on ultra-wideband real-time locating system. In: IEEE/ASME International Conference on Advanced Intelligent Mechatronics, 2009, pp. 1359–1364 (2009)
16. Wang, B., Toobaei, M., Danskin, R., Ngarmnil, T., Pham, L., Pham, H.: Evaluation of RFID and Wi-Fi technologies for RTLS applications in healthcare centers. In: 2013 Proceedings of PICMET '13 Technology Management in the IT-Driven Services, pp. 2690–2703 (2013)
17. Yao W., Chu, C.-H., Li, Z.: The use of RFID in healthcare: benefits and barriers. In: 2010 IEEE International Conference on RFID-Technology and Applications (RFID-TA), pp. 128–134 (2010)
18. Bhattacharya, M., Chu, C.-H., Hayya, J., Mullen, T.: An exploratory study of RFID adoption in the retail sector. Oper. Manag. Res. **3**(1–2), 80–89 (2010)
19. Segovis, P.: Drive savings with mobile asset management. Health Manag. Technol. (2012). Available: http://www.healthmgttech.com/articles/201211/drive-savings-with-mobile-asset-management.php
20. Kotzen, M.S.: N.J. health system saves $1.2 million. Health Manag. Technol. (2013). Available: http://www.healthmgttech.com/articles/201308/nj-health-system-saves-12-million.php
21. Sewdberg, C.: Mexican state agency reduces donated blood wastage with RFID. RFID J. (2014). http://www.rfidjournal.com/articles/view?12440
22. Becker, E., Metsis, V., Arora, R., Vinjumur, J., Xu, Y., Makedon, F.: SmartDrawer: RFID-based smart medicine drawer for assistive environments. In: Proceedings of the 2nd International Conference on Pervasive Technologies Related To Assistive Environments (PETRA '09), pp. 1–9 (2009)
23. Vinjumur, J.K., Becker, E., Ferdous, S., Galatas, G., Makedon, F.: Web based medicine intake tracking application. In: Proceedings of the 3rd International Conference on Pervasive Technologies Related to Assistive Environments (2010)
24. Hasanuzzaman, F.M., Tian, Y.L., Liu, Q.: Identifying medicine bottles by incorporating RFID and video analysis. In: 2011 IEEE International Conference on Bioinformatics and Biomedicine Workshops (BIBMW), pp. 528–529 (2011)
25. Rajagopalan, H., Rahmat-Samii, Y.: Ingestible RFID bio-capsule tag design for medical monitoring. In: 2010 IEEE Antennas and Propagation Society International Symposium (APSURSI), pp. 1–4 (2010)
26. Polycarpou, A.C., Dimitriou, A., Bletsas, A., Polycarpou, P.C., Papaloizou, L., Gregoriou, G., Sahalos, J.N.: On the design, installation, and evaluation of a radio-frequency identification system for healthcare applications. IEEE Antennas Propag. Mag. **54**(4), 255–271 (2012)
27. Castro, L., Lefebvre, E., Lefebvre, L.: Adding intelligence to mobile asset management in hospitals: the true value of RFID. J. Med. Syst. **37**(5), 1–17 (2013)
28. Zhao, Y., Zhou, H., Li, M.: WiTracker: an indoor positioning system based on wireless LANs. In: 2010 6th International Conference on Wireless Communications Networking and Mobile Computing (WiCOM), pp. 1–4 (2010)
29. Au, A.W.S., Feng, C.; Valaee, S., Reyes, S., Sorour, S., Markowitz, S.N., Gold, D., Gordon, K., Eizenman, M.: Indoor tracking and navigation using received signal strength and compressive sensing on a mobile device. IEEE Trans. Mob. Comput. **12**(10), 2050–2062 (2013)
30. Zhang, D., Zhou, J., Guo, M., Cao, J., Li, T.: TASA: tag-free activity sensing using RFID tag arrays. IEEE Trans. Parallel Distrib. Syst. **22**(4), 558–570 (2011)
31. Chen, R.-C., Lin, Y.-H.: Apply Kalman filter to RFID Received Signal Strength processing for indoor location. In: 2012 4th International Conference on Awareness Science and Technology (iCAST), pp. 73–77, 21–24 (2012)

32. Zhao, J., Zhang, Y., Ye, M.: Research on the received signal strength indication location algorithm for RFID system. In: International Symposium on Communications and Information Technologies, 2006. ISCIT '06, pp. 881–885 (2006)
33. Huang, Y., Brennan, P.V., Seeds, A.: Active RFID location system based on time-difference measurement using a linear FM chirp tag signal. In: IEEE 19th International Symposium on Personal, Indoor and Mobile Radio Communications, 2008. PIMRC 2008, pp. 1–5 (2008)
34. Zou, Z., Deng, T., Zou, Q., Sarmiento, M.D., Jonsson, F., Zheng, L.-R.: Energy detection receiver with TOA estimation enabling positioning in passive UWB-RFID system. In: 2010 IEEE International Conference on Ultra-Wideband (ICUWB), vol. 2, pp. 1–4 (2010)
35. Zhai, C., Zou, Z., Zhou, Q., Zheng, L.: A software defined radio platform for passive UWB-RFID localization. In: 2012 IEEE International Conference on Wireless Information Technology and Systems (ICWITS), pp. 1–4 (2012)
36. Ai, Z., Liu, Y.: Research on the TDOA measurement of active RFID real time location system. In: 2010 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT), vol. 2, pp. 410–412 (2010)
37. Azzouzi, S., Cremer, M., Dettmar, U., Kronberger, R., Knie, T.: New measurement results for the localization of UHF RFID transponders using an Angle of Arrival (AoA) approach. In: 2011 IEEE International Conference on RFID, pp. 91–97 (2011)
38. Hua, M-C., Peng, G.-C. Lai, Y.J., Liu, H.-C.: Angle of arrival estimation for passive UHF RFID tag backscatter signal. In: IEEE International Conference on and IEEE Cyber, Physical and Social Computing Green Computing and Communications (GreenCom), 2013 IEEE and Internet of Things (iThings/CPSCom), pp. 1865–1869 (2013)
39. Toplan, E., Ersoy, C.: RFID based indoor location determination for elderly tracking. In: 20th Signal Processing and Communications Applications Conference (SIU), pp. 1–4 (2012)
40. Sutherland, J., van den Heuvel, W.-J.: Towards an intelligent hospital environment: adaptive workflow in the OR of the future. In: Proceedings of the 39th Annual Hawaii International Conference on System Sciences, 2006, HICSS '06, vol. 5, pp. 100b (2006). doi:10.1109/HICSS.2006.494
41. Okoniewska, B., Graham, A., Gavrilova, M., Wah, D., Gilgen, J., Coke, J., Burden, J. Nayyar, S., Kaunda, J., Yergens, D., Baylis, B. Ghali, W.A.: Multidimensional evaluation of a radio frequency identification Wi-Fi location tracking system in an acute-care hospital setting. J. Am. Med. Inform. Assoc. **19**(4), 674–679 (2012)
42. Arcega, L., Font, J., Cetina, C.: Towards memory-aware services and browsing through lifelogging sensing. Sensors **13**(11), 15113–15137 (2013)
43. Blasco, R., Marco, Á., Casas, R., Cirujano, D., Picking, R.: A smart kitchen for ambient assisted living. Sensors **14**(1), 1629–1653 (2014)
44. Wang, S.-W., Chen, W.-H., Ong, C.-S., Liu, L., Chuang, Y.-W.: RFID application in hospitals: a case study on a demonstration RFID project in a Taiwan hospital. In: Proceedings of the 39th Annual Hawaii International Conference on System Sciences, vol. 8, pp. 184a (2006)
45. Hanser, F., Gruenerbl, A., Rodegast, C., Lukowicz, P.: Design and real life deployment of a pervasive monitoring system for dementia patients. In: Second International Conference on Pervasive Computing Technologies for Healthcare, pp. 279–280 (2008)
46. Lee, S.-Y., Cho, G.-S.: A simulation study for the operations analysis of dynamic planning in container terminals considering RTLS. In: Second International Conference on Innovative Computing, Information and Control (ICICIC '07), pp. 116 (2007)
47. Cangialosi, A., Monaly, J.E., Yang, S.C.: Leveraging RFID in hospitals: patient life cycle and mobility perspectives. IEEE Commun. Mag. **45**(9), 18–23 (2007)
48. Xiong, J., Seet, B.-C., Symonds, J.: Human activity inference for ubiquitous RFID-based applications. In: 2009 Symposia and Workshops on Ubiquitous, Autonomic and Trusted Computing, pp. 304–309 (2009)
49. Saygin, C.: Adaptive inventory management using RFID data. Int. J. Adv. Manuf. Technol. **32**(9–10), 1045–1051 (2007)
50. Goebel, C., Günther, O.: Benchmarking RFID profitability in complex retail distribution systems. Electron. Mark. **19**(2–3), 103–114 (2009)

51. Bustillo, M.: Wal-Mart radio tags to track clothing. Wall Street J. July 23, 2010. http://www.wsj.com/articles/SB10001424052748704421304575383213061198090
52. Shieh, H.-L., Lin, S.-F., Chang, W.-S.: RFID medicine management system. In: 2012 International Conference on Machine Learning and Cybernetics (ICMLC), vol. 5, pp. 1890–1894 (2012)
53. Juels, A.: 2006. RFID security and privacy: a research survey. IEEE J. Sel. Areas Commun. **24**(2), 381–394 (2006)
54. Garfinkel, S.L., Juels, A., Pappu, R.: RFID privacy: an overview of problems and proposed solutions. IEEE Secur. Priv. **3**(3), 34–43 (2005)
55. Lee, Y.K., Batina, L., Singelée, D., Verbauwhede, I.: Low-cost untraceable authentication protocols for RFID. In: Proceedings of the Third ACM Conference on Wireless Network Security (WiSec '10), pp. 55–64 (2010)
56. Li, Y., Teraoka, F.: Privacy protection for low-cost RFID tags in IoT systems. In: Proceedings of the 7th International Conference on Future Internet Technologies (CFI '12), pp. 60–65 (2012)
57. Engels, D.W., Kang, Y. S., Wang, J.: On security with the new Gen2 RFID security framework. In: 2013 IEEE International Conference on RFID, pp. 144–151 (2013)
58. Karjoth, G., Moskowitz, P.A.: Disabling RFID tags with visible confirmation: clipped tags are silenced. In: Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society (WPES '05), pp. 27–30 (2005)
59. Barlow, R.: Next-generation tracking: go beyond tracking people, products and equipment. Health Manag. Technol. **35**(10), 6–11 (2014)
60. Hart, C., Hawrylak, P.J.: Using radio frequency identification (RFID) tags to store medical information needed by first responders: data format, privacy, and security. Int. J. Comput. Methods Algorithms Med. **3**(3), 10–26 (2012)