University of Canberra
School of Information Science & Engineering
Information Sciences Ext Studies PG 4421

Health Care Patient Management
A Wireless Framework

Omar Sultan Al-Kadi*
November 3, 2003

*o.alkadi@student.canberra.edu.au

Table of Contents

Abstract 1
Introduction 1
RFID Background 1
Definition of RFID 1
RFID main components 2
Types of RFID Transponders (tags) 2
Active Tags 3
Passive Tags 3
Range 4
Low frequency range 4
High frequency range 4
Shapes of RFID tags 4
Transceivers 5
RFID Transponder Programmers 5
Practical Cases using RFID technology 6
Case I: Acquisition of Patient's Medical Data 6
Case II: Locating the nearest available doctor to the patients location 8
Case III: Doctors stimulates the patient's active RFID tag using their PDAs in order to acquire the medical data stored in it. 12
Maintaining Patients' Data Security and Integrity 14
Layers of encryption 14
Physical (hardware) layer encryption 14
Application (software) layer encryption 14
Framework of Encrypting Patient's Medical Data 14
Choosing level of security for the wirelessly-transmitted medical data 18
Conclusion 18
References 19

Table of Figures

Figure 1: Managing health care data using a wireless framework 7
Figure 2 Acquisition of patient's medical data 10
Figure 3 Locating the nearest available doctor to the patient's location 11
Figure 4 Interrogating patient's data using RFID transceiver-tag technology 14
Figure 5: Patient's medical data Encryption framework 16
Figure 6: Choosing level of security for the wirelessly-transmitted medical data 17

Abstract

When dealing with human lives, which are considered the most valuable thing as compared to other materialistic matters, emerges the need to utilize and apply the latest technology to help in saving and also maintaining patient's lives. Hence comes the issue of delivering patient's medical data as fast and as secure as possible. Thus, a wireless framework based on radio frequency identification (RFID) integrated with wireless networks were chosen for fast data acquisition and transmission, while the security issue is discussed in details to overcome any vulnerability.

Introduction

Radio Frequency Identification (RFID) is a new and promising technology which could expand and penetrate many fields of application in today and in the near future. Thus, RFID is used as a base for this research report in managing patients' health care data in a wireless and paperless hospital environment. Nevertheless, RFID needs to operate and integrate with other available wireless technologies as the IEEE 802.11b, in order to fulfill its requirements effectively and efficiently.

This research report is divided into three main sections. The first section is a RFID background, which will give a brief definition of RFID and its main components. This section also discusses which types of RFID components are most suitable for the hospital environment and how they can be placed. The second section is about practical cases using the RFID technology. The second section lists three possible applicable cases assisting in managing patients' medical data and determining doctor's location. The final and third section discusses the important issue of maintaining patients' data security and integrity

RFID Background

This part will shed some light on various types of RFID components; through explaining out of what does an RFID system consists. Following that, this section will discuss what components of the RFID technology are suitable for hospitals and medical centers- depending on type, shape, frequency bandwidth and range.

Definition of RFID

RFID is a flexible technology that is convenient, easy to use, and well suited for automatic operation. It combines advantages not available with other identification technologies. RFID can be supplied as read-only or read/write, does not require contact or line-of-sight to operate, can function under a variety of environmental conditions, and provides a high level of data integrity [1].

RFID main components

A basic RFID system consists of three main components:

1. ***Antenna or coil***;
2. ***Transceiver*** (with decoder);
3. ***Transponder*** (RFID tag) which can be on-line or off-line electronically programmed with unique information.

The antenna emits radio signals to activate the tag and read and write data to it. Antennas are the conduits between the tag and the transceiver, which controls the system's data acquisition and communication. Antennas are available in many shapes and sizes; they can be built into a doorframe to receive tag data from persons or things passing through the door, or mounted on a tollbooth to monitor traffic passing by on a freeway [2].

Often the antenna is packaged with the transceiver and decoder to become a reader, which can be configured either as a handheld or a fixed-mount device. For our case, in order to manage medical data we need both types- fixed and handheld transceivers, by placing fixed transceivers in biomedical devices located in ICUs and CCUs. Also, transceivers can be assembled in ward ceilings or door frames to collect and disseminate patient's medical data. Moreover, we need portable or handheld transceivers so that physicians can retrieve the patient's medical data stored in transponders (RFID tags) once they stand beside their beds or enter the ward.

The reader emits radio waves in ranges of anywhere from one inch to 33 meters or more, depending upon its power output and the radio frequency used which will be discussed in the next part of this section. In respect of transponders (RFID tags), when these tags passes through the electromagnetic zone, they detect the reader's activation signal. Then the reader decodes the data encoded in the tag's integrated circuit and the data is examined by the physician or passed to the hospitals server for storage.

The next subsection discusses RFID tags. By displaying how they differ in type, shape, range and frequency bandwidth, which depends on their particular use. Also, some recommendations will be given indicating which are more suitable for the medical environment.

Types of RFID Transponders (tags)

RFID tags are categorized as either active or passive. Therefore, the condition of the application place and use determines the required tag type. First, a definition will be given for each type, and then the required tag which suits best our application will be chosen.

Active Tags

Active RFID tags are powered by an internal battery and are typically read/write, i.e., tag data can be rewritten and/or modified. An active tag's memory size varies according to application requirements; some systems operate with up to 1MB of memory. In a typical read/write RFID work-in-process system, a tag might give a machine a set of instructions, and the machine would then report its performance to the tag. This encoded data would then become part of the tagged part's history. The battery-supplied power of an active tag generally gives it a longer read range. The trade off is greater size, greater cost, and a limited operational life (which may yield a maximum of 10 years, depending upon operating temperatures and battery type) [2].

Passive Tags

Passive RFID tags operate without a separate external power source and obtain operating power generated from the reader. Passive tags are consequently much lighter than active tags, less expensive, and offer a virtually unlimited operational lifetime. The trade off is that they have shorter read ranges than active tags and require a higher-powered reader. Read-only tags are typically passive and are programmed with a unique set of data (usually 32 to 128 bits) that cannot be modified. Read-only tags most often operate as a license plate into a database, in the same way as linear barcodes reference a database containing modifiable product-specific information [2].

After examining both types, we can suggest the following:

- It is more suitable to embed the RFID transponders (tags) in wrist bands instead of embedding them in the patient's own custom.
- Doctors should have RF tags embed in their PDAs. This enables them to retrieve the patient's medical data directly whenever they are near the patient, instead of waiting until the medical data is pushed to them through the hospital server.
- *Active RFID tags* are the one required for collection of the patient's medical data. Since the medical data needs to be continuously recorded to the patient's hand wrist RFID tag to be then sent to the RFID reader. This will cause for the RFID tag to be a bit bulky because of the needed battery for the write process. However, this is the only way to recorder the medical data on real-time (online) bases using the RFID technology, and size could decrease as technology advances.
- *Passive RFID tags* can be also used as well. These passive tags can be embedded in the doctors PDA, which is needed for determining their locations whenever the medical staff requires them. Also, passive tags can be used in patients' wrist bands for storage of limited amount of data- on offline bases, e.g. date of hospital admission, medical record number, etc.

Range

RFID systems are also distinguished by their frequency ranges. This in turn depends on their particular use and where they need to be deployed. RFID transponders (tags) operated in two different types of frequencies, which make them adaptable for nearly any application. These ranges are:

Low frequency range

Low-frequency (30 KHz to 500 KHz) systems have short reading ranges and lower system costs. They are most commonly used in security access, asset tracking, and animal identification applications [3].

High frequency range

High-frequency (850 MHz to 950 MHz and 2.4 GHz to 2.5 GHz) systems, offering long read ranges (greater than 33 meters) and high reading speeds, are used for such applications as railroad car tracking and automated toll collection. However, the higher performance of high-frequency RFID systems incurs higher system costs [3].

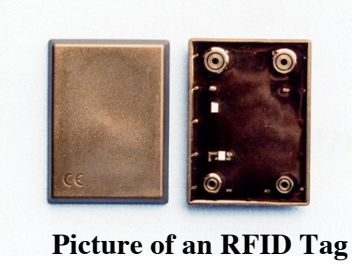
After examining both ranges, we can suggest the following:

- *Low frequency range tags* are suitable for the patients' band wrist RFID tags. Since we expect that the patients' bed is not too far from the RFID reader, which might be fixed on the room ceiling or door-frame. Also the doctor aiming to read the patient's data directly through his PDA would be in the same room.
- *High frequency range tags* are suitable for the physician's tag implanted in their PDAs. As physicians use to move from on location to another in the hospital.

However, one final point regarding RFID range is that until now the permissible RF range is not regulated, i.e., it still operates in some low frequency ranges (30- 500 KHz) and in the free 2.45 GHz ISM (Industry, Science and Medical) band of frequency, which the IEEE's 802.11b (WiFi) wireless networks also operates in, and many other wireless application. This band of frequency is already crowded, which certainly will slow the speed of RF signal transmission.

Shapes of RFID tags

RFID tags come in a wide variety of shapes and sizes. Animal tracking tags, inserted beneath the skin, can be as small as a pencil lead in diameter and one centimeter in length. Tags can be screw-shaped to identify trees or wooden items, or credit-card shaped for use in access applications. The anti-theft hard plastic tags attached to merchandise in stores are also RFID tags. [2].



Picture of an RFID Tag (courtesy CopyTag limited) [5]

Transceivers

The transceivers/interrogators can differ quite considerably in complexity, depending upon the type of tags being supported and the functions to be fulfilled. However, the overall function is to provide the means of communicating with the tags and facilitating data transfer. Functions performed by the reader may include quite sophisticated signal conditioning, parity error checking and correction. Once the signal from a transponder has been correctly received and decoded, algorithms may be applied to decide whether the signal is a repeat transmission, and may then instruct the transponder to cease transmitting. This is known as the "Command Response Protocol" and is used to circumvent the problem of reading multiple tags in a short space of time. Using interrogators in this way is sometimes referred to as "Hands Down Polling". An alternative, more secure, but slower tag polling technique is called "Hands Up Polling" which involves the transceiver looking for tags with specific identities, and interrogating them in turn. A further approach may use multiple transceivers, multiplexed into one interrogator, but with attendant increases in costs [2, 3, and 4].

For our case, since we deal with sensitive and critical information (patient's medical data), we need the *Hands Down polling* techniques in conjunction with multiple transceivers which are multiplexed with each other forming a wireless network. The reason behind my choice is that, we need high speed for transferring medical data from medical equipments to the RFID wrist band tag to the nearest RFID reader. Then through a wireless network or a network of RFID transceivers to the hospital server, to be then transmitted to the doctor's PDA or laptop through a WLAN- an IEEE 802.11b which operated at the 5.2 GHz band at a data transfer rate of 54 Mbps, or through the latest IEEE 802.11g operating at the same speed as the IEEE 802.11a but working at the free ISM band.

The Hand Down Polling techniques, as previously described, provides the ability to detect all detectable RFID tags at once (i.e. in parallel). Preventing any unwanted delay in transmitting medical data corresponding to each RF tagged patient.

RFID Transponder Programmers

Transponder programmers are the means, by which data is delivered to write once, read many (WORM) and read/write tags. Programming can be carried out off-line or on-line. For some systems re-programming may be carried out on-line, particularly if it is being used as an interactive portable data file within a production environment, for example. Data may need to be recorded during each process. Removing the transponder at the end of each process to read the previous process data, and to program the new data, would naturally increase process time and would detract substantially from the intended flexibility of the application. By combining the functions of a transceiver and a programmer, data may be appended or altered in the transponder as required, without compromising the production line [2].

We conclude from this section that RFID systems differ in type, shape, and range; depending on the type of application, the RFID components shall be chosen. Low frequency range tags are suitable for the patients' band wrist RFID tags. Since we expect that the patients' bed is not too far from the RFID reader, which might be fixed on the room ceiling or door-frame. High frequency range tags are suitable for the physician's PDA tag. As physicians use to move from on location to another in the hospital, long read ranges are required. On the other hand, transceivers which deal with sensitive and critical information (patient's medical data) need the Hands Down polling techniques. These multiple transceivers should be multiplexed with each other forming a wireless network.

Practical Cases using RFID technology

This section explains in details three possible applications of the RFID technology in three applicable cases. Each case is discussed step-by-step then represented by a flowchart. Those cases cover issues as acquisition of Patient's Medical Data, locating the nearest available doctor to the patients location, and how doctors stimulate the patient's active RFID tag using their PDAs in order to acquire the medical data stored in it.

Starting by depicting my own perspective (see figure 1) of the wireless framework of managing patient's data, on which this report will be based on.

Case I: Acquisition of Patient's Medical Data

Case one will represent the method of acquisition and transmission of medical data. This process can be described in the following points as follows:

1) A biomedical device equipped with an embedded RFID transceiver and programmer will detect and measure the biological state of a patient. This medical data can be an ECG, EEG, BP, sugar level, temperature or any other biomedical reading.

After the acquisition of the required medical data, the biomedical device will write -burn this data to the RFID transceiver's EEPROM using the built in RFID programmer. Then the RFID transceiver with its antenna will be used to transmit the stored medical data in the EEPROM to the EEPROM in the patient's transponder (tag) which is around his/her wrist. The data received will be updated periodically once new fresh readings are available by the biomedical device. Hence, the newly sent data by the RFID transceiver will be accumulated to the old data in the tag. The purpose of the data stored in the patient's tag is to make it easy for the doctor to obtain medical information regarding the patient directly via the doctor's PDA, tablet PC or laptop[1].

[1] more on this issue will be discussed in case no.3 in this section.

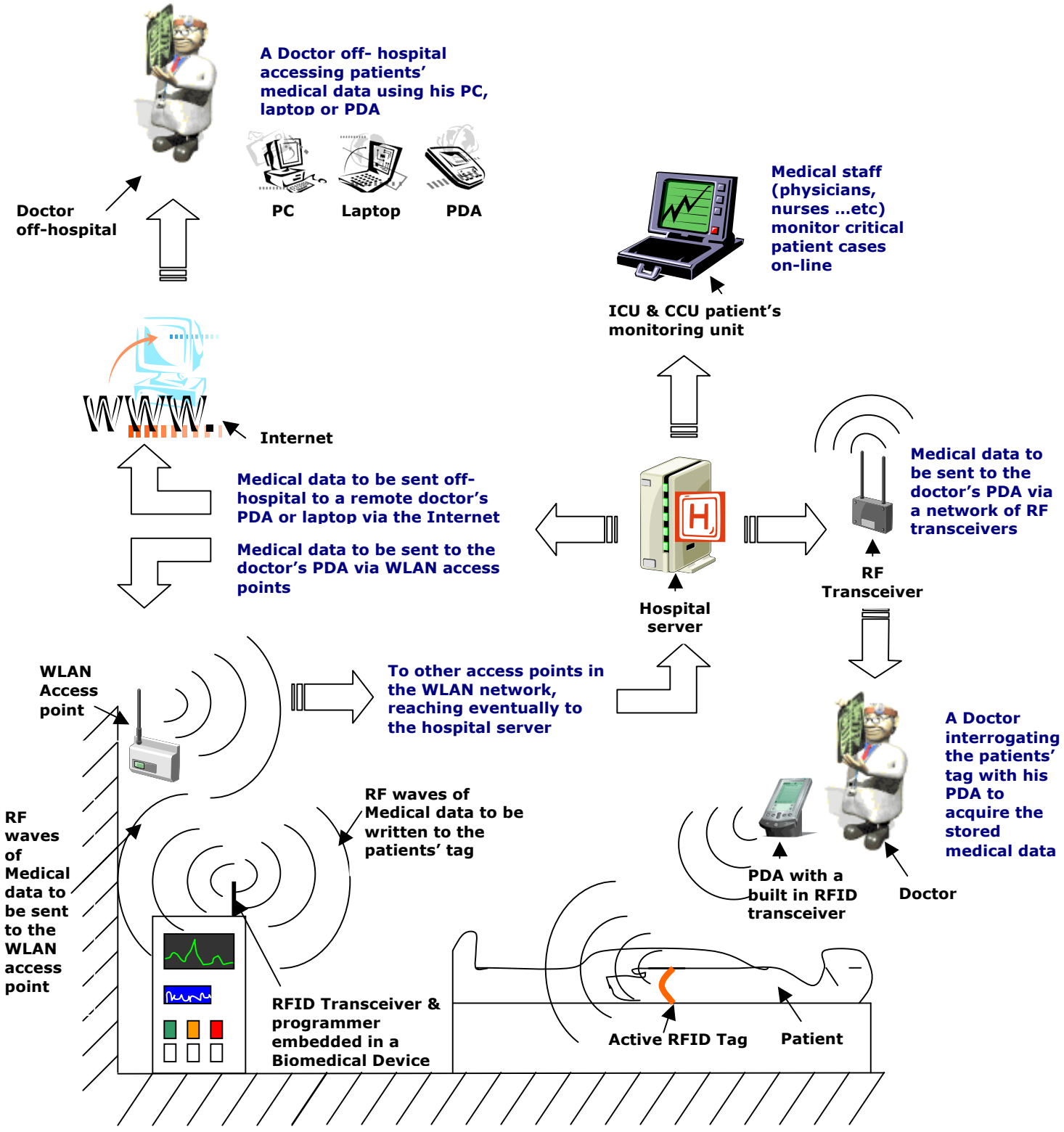


Figure 1: Managing health care data using a wireless framework

2) Similarly, the biomedical device will also transfer the measured medical data wirelessly to the nearest WLAN access point. Since high data rate transfer rate is crucial in transferring medical data, IEEE 802.11b or g is recommended for the transmission purpose.

3) Then the wirelessly sent data will be routed to the hospitals main server; to be then sent (pushed) to:

i) Other doctors available throughout the hospital so they can be notified of any newly received medical data.

ii) To an on-line patient monitoring unit or a nurse's workstation within the hospital.

iii) Or the acquired patients' medical data can be fed into an expert (intelligent) software system running on the hospital server. To be then compared with other previously stored abnormal patterns of medical data, and to raise an alarm if any abnormality is discovered[2].

4) Another option could be using the in-built-embedded RFID transceiver in the biomedical device to send the acquired medical data wirelessly to the nearest RFID transceiver in the room. Then the data will travel simultaneously in a network of RFID transceivers until reaching the hospital server (see flowchart, figure 2).

Case II: Locating the nearest available doctor to the patients location

This case will explain how to locate the nearest doctor who is needed urgently to attend an emergency medical situation. This case can be explained as follows:

1) If a specific surgeon or physician is needed in a specific hospital department, the medical staff in the monitoring unit (e.g. nurses) can query the hospital server for the nearest available doctor to the patient's location.

2) The hospital server traces all doctors' locations in the hospital through detecting the presences of their wireless mobile device; e.g. PDA, tablet PC or laptop in the WLAN range.

3) Another method that the hospital's server can use to locate the physicians is making use of the RFID transceivers built-in the doctor's wireless mobile device. Similarly to the access points used in WLAN, RFID transceivers can assist in

[2] See flowchart of case no.2

serving a similar role of locating doctor's location. This can be described in three steps, which are:

i) The fixed RFID transceivers throughout the hospital will send a stimulation signal to detect other free RFID transceivers – which are in the doctors PDAs, tablets or laptops, etc.[3]

ii) Then all free RFID transceivers will receive the stimulation signal and reply back with an acknowledgement signal to the nearest fixed RFID transceiver.

iii) Finally, each free RFID transceiver cell position would be determined by locating to which fixed RFID transceiver range it belongs to or currently operating in.

4) After the hospital server located positions of all available doctors, it determines the nearest requested physician (pediatrics, neurologist …etc) to the patient's location.

5) Once the required physician is located, an alert message will be sent to his\her PDA, tablet PC or laptop indicating the location to be reached immediately. This alert message could show:

i) The building, floor and room of the patient (e.g. 3C109).

ii) Patient's case (e.g. heart stroke, arrhythmia, etc…)

iii) A brief description of the patient's case.

6) If the hospital is running an intelligent medical expert software system on its server, the process of locating and sending an alert message can be automated. This is done through comparing the collected medical data with previously stored abnormal patterns of medical data, then sending an automated message describing the situation. This system could be used instead of the staff in the patient monitoring unit or the nurse's workstation who observe and then sending an alert message manually.

Figure 3 demonstrates the whole case in a flowchart involving both situations- automated and manually, for patient abnormality detection and doctor position determination.

[3] *Fixed RFID* transceivers are the transceivers fixed on the walls and door- frames throughout the hospital. They serve as a wireless network for transmitting medical data from the *free RFID* transceivers which are built-in doctor's wireless mobile devices (PDAs, tablet PCs and laptops) to the hospital server and vice versa.

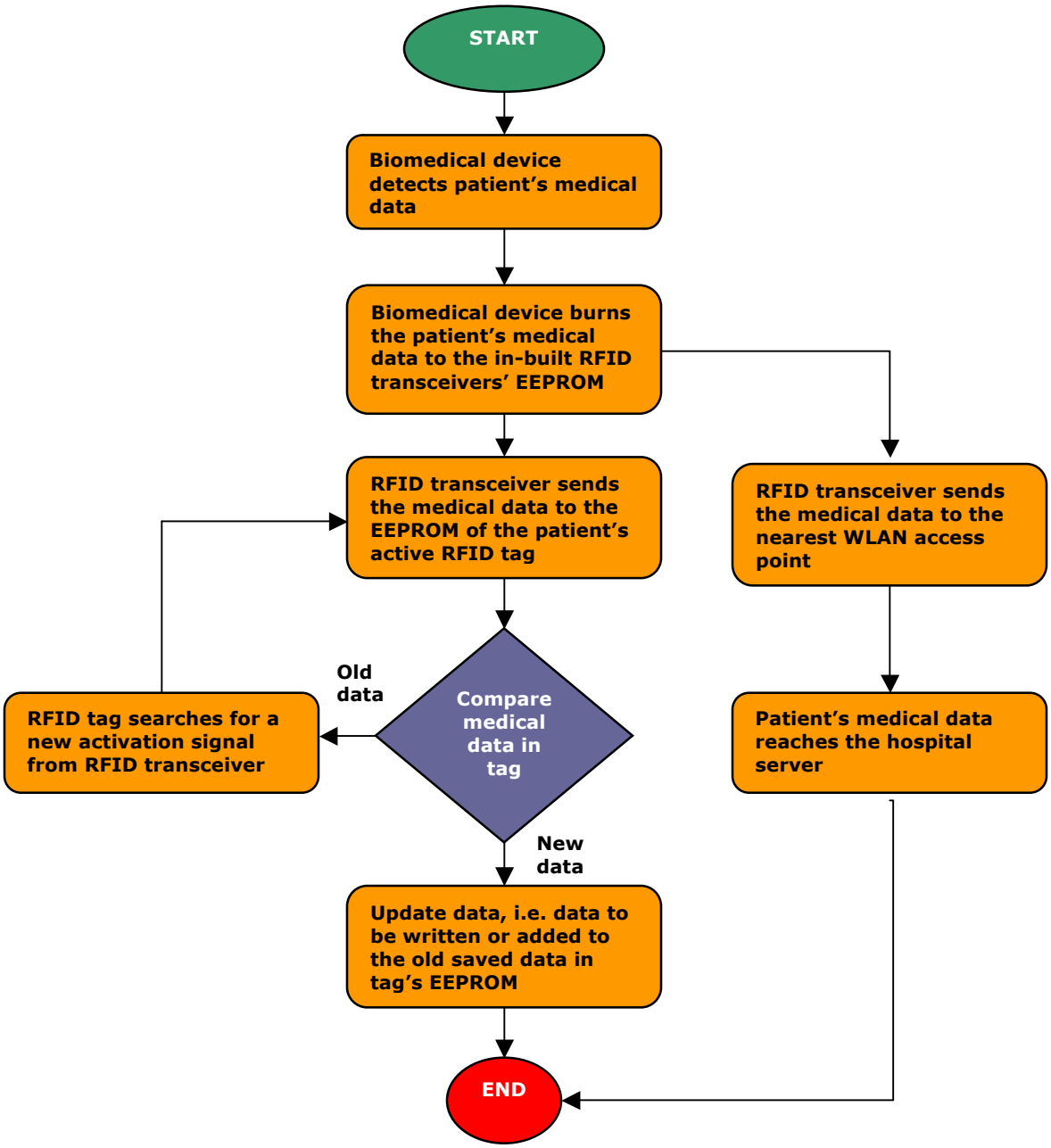


Figure 2 Acquisition of patient's medical data

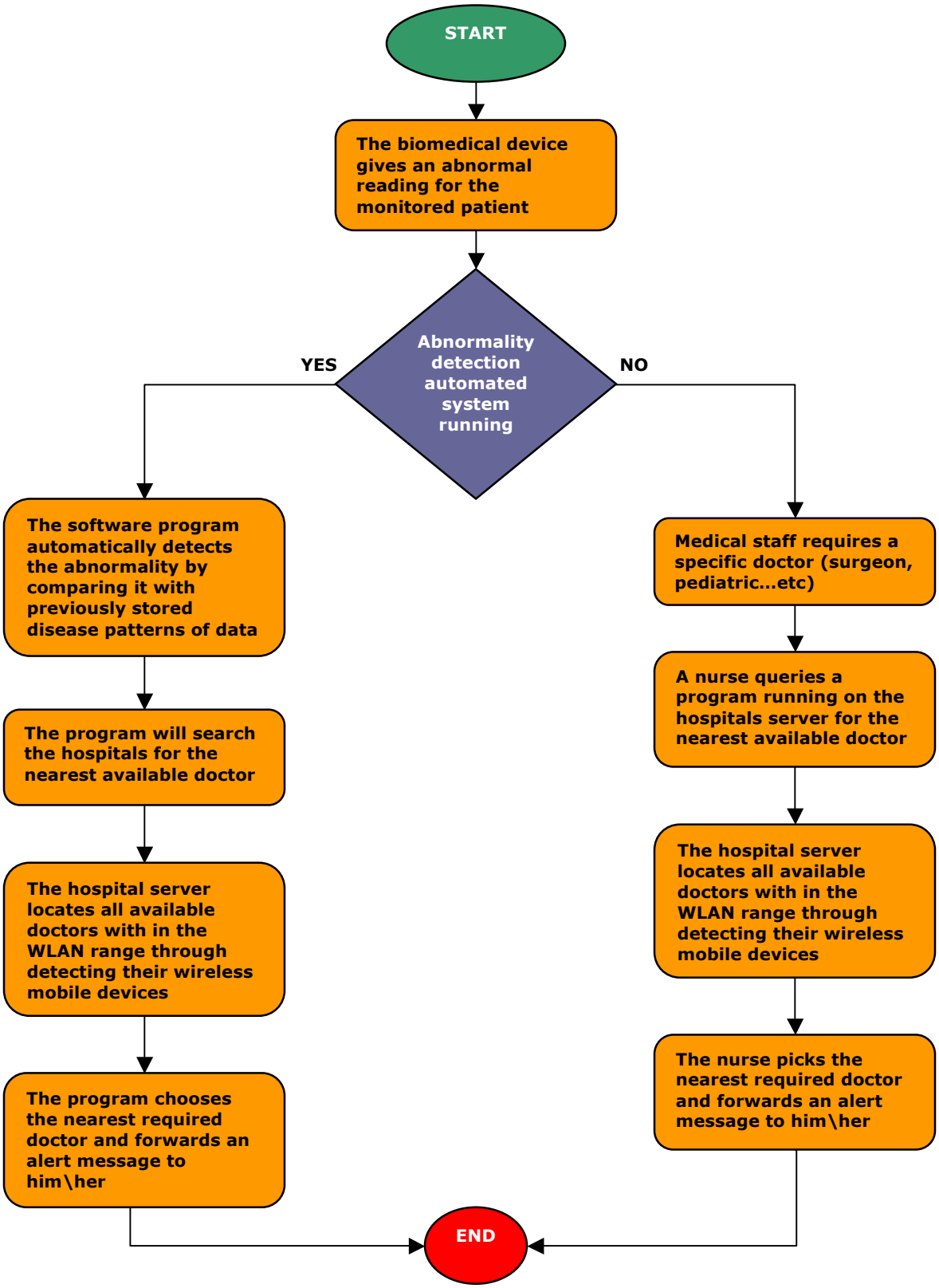


Figure 3 Locating the nearest available doctor to the patient's location

Case III: Doctors stimulates the patient's active RFID tag using their PDAs in order to acquire the medical data stored in it.

This method can be used in order to get rid of medical files and records placed in front of the patient's bed. Additionally, it could help in preventing medical errors- reading the wrong file for the wrong patient- and could be considered as an important step towards a paperless hospital.

This case can be described in the following steps:

1) The doctor enters into the patient's room or ward. The doctor wants to check the medical status of a certain patient. So instead of picking up the 'hard' paper medical file, the doctor interrogates the patient's RFID wrist tag with his RFID transceiver equipped in his\her PDA, tablet PC or laptop, etc.

2) The patient's RFID wrist tag detects the signal of the doctor's RFID transceiver coming from his\her wireless mobile device and replies back with the patient's information and medical data.

3) If there was more than one patient in the ward possessing RFID wrist tags, all tags can respond in parallel using Hands Down polling techniques[4] back to the doctor's wireless mobile device.

4) Another option could be, the doctor retrieving only the patient's number from the *passive* RFID wrist tag. Then through the WLAN the doctor could access the patient's medical record from the hospital's main server (see flowchart in figure 4 next page).

RFID technology has many potential important applications in hospitals, and the discussed three cases are a real practical example. Two important issues can be concluded from this section: WLAN is preferred for data transfer; given that IEEE's wireless networks have much faster speed and coverage area as compared to RFID transceivers\ transponders technology. Yet, RFID technology is the best for data storage and locating positions of medical staff and patients as well.

The other point is that we need a RFID Transceiver & programmer embedded in a Biomedical Device for data acquisition and dissemination, and only a RFID Transceiver embedded in the doctor's wireless mobile device for obtaining the medical data. With the progress the RFID technology is currently gaining, it could become standard as other wireless technologies (Bluetooth for example), and eventually manufacturers building them in electronic devices; biomedical devices for our case.

[4] refer to RFID Background section in this report under title Transceivers for more information on Hands Down polling techniques

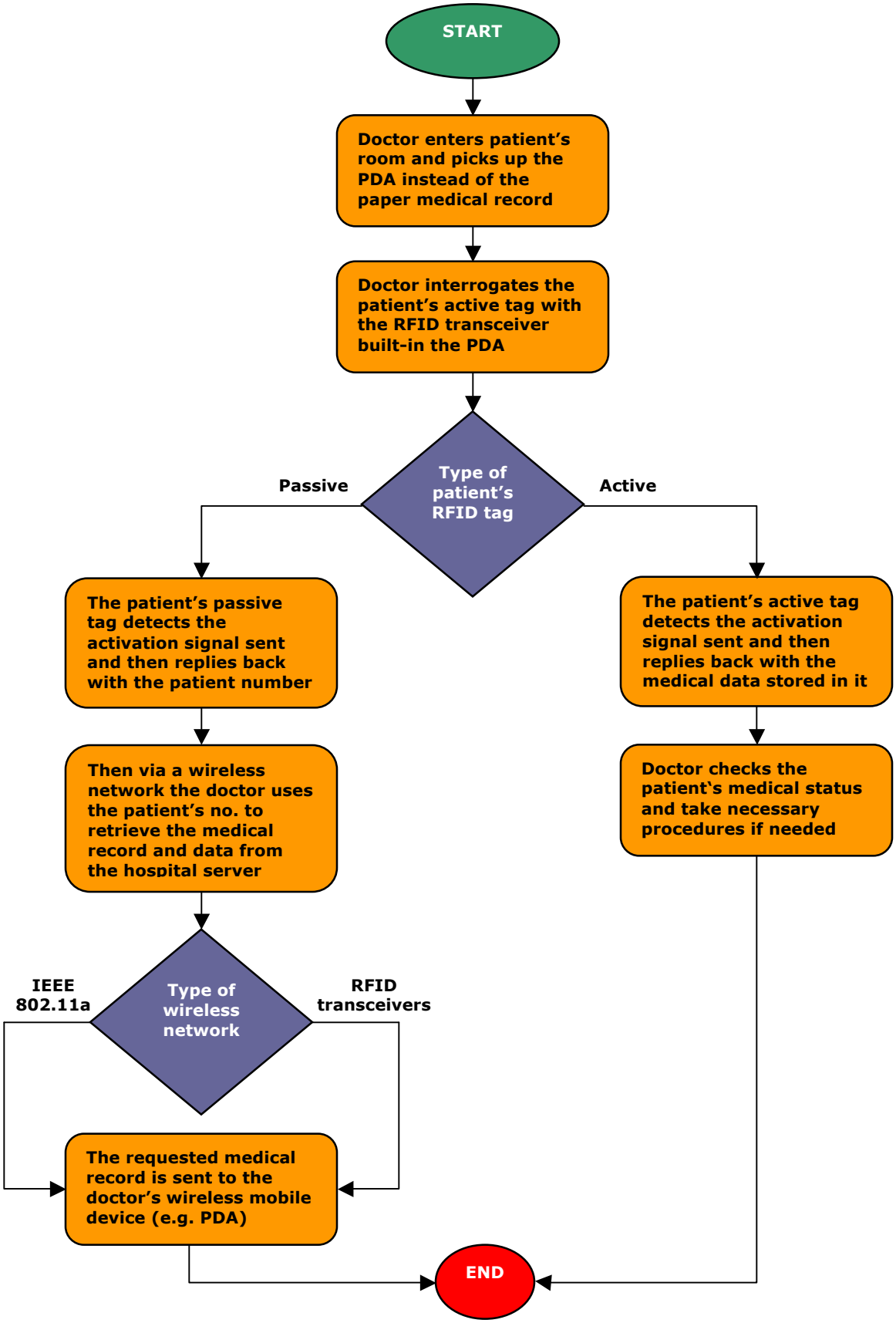

START
Doctor enters patient's room and picks up the PDA instead of the paper medical record
Doctor interrogates the patient's active tag with the RFID transceiver built-in the PDA
Type of patient's RFID tag
Passive
Active
The patient's passive tag detects the activation signal sent and then replies back with the patient number
The patient's active tag detects the activation signal sent and then replies back with the medical data stored in it
Then via a wireless network the doctor uses the patient's no. to retrieve the medical record and data from the hospital server
Doctor checks the patient's medical status and take necessary procedures if needed
Type of wireless network
IEEE 802.11a
RFID transceivers
The requested medical record is sent to the doctor's wireless mobile device (e.g. PDA)
END

Figure 4 Interrogating patient's data using RFID transceiver-tag technology

Maintaining Patients' Data Security and Integrity

Once data is transmitted wirelessly, security becomes a crucial issue. Unlike wired transmission, wirelessly transmitted data can be easily sniffed out leaving the transmitted data vulnerable to many types of attacks. For example, wireless data could be easily eavesdropped on using any mobile device equipped with a wireless card. In worst cases wirelessly transmitted data could be intercepted and then possibly tampered with, or in best cases, the patient's security and privacy would be compromised. Hence emerges the need for data to be initially encrypted from the source.

This section of the report discusses how we could apply encryption to the designed wireless framework which was explained in the previous section. This is done by suggesting exactly where data needs to be encrypted and\or decrypted depending on the case that is being examined.

First a definition of the type of encryption that would be used in the design of the security (encryption\decryption) framework is discussed, and then followed by a flowchart demonstrating the framework in a step-by-step process.

Layers of encryption

Two main layers of encryption are recommended to be used, they are:

Physical (hardware) layer encryption

This means encrypting all collected medical data at the source or hardware level before transmitting it. Thus, we insure that the patient's medical data would not be compromised once exposed to the outer world on its way to its destination. So even if a person with a malicious intent and also possessing a wireless mobile device steps into the coverage range of the hospitals' WLAN, this intruder will gain actually nothing since all medical data is encrypted, making all intercepted data worthless.

Application (software) layer encryption

This means encrypting all collected medical data at the destination or application level once receiving it. Application level encryption runs on the doctor's wireless mobile device (e.g. PDA, tablet PC or laptop) and on the hospital server. Once the medical data is received, it will be protected by a secret pass-phrase (encryption\decryption key) created by the doctor who possesses this device. This type of encryption would prevent any person from accessing patient's medical data if the doctor's wireless mobile device gets lost, or even if a hacker hacks into the hospital server via the Internet, intranet or some other mean.

Framework of Encrypting Patient's Medical Data

The previous section (Practical Cases using RFID Technology) focused on how to design a wireless framework to reflect how patient's medical data can be managed efficiently and effectively leading to the elimination of errors, delays and even paperwork. Similarly, this section will focus on the previously discussed framework from a security perspective, attempting to increase security and data integrity.

Figure 5 demonstrates two of the three cases discussed in the past report that involved transmitting and\or receiving patient's medical data, they are:

i) acquisition of Patient's Medical Data
ii) Doctors stimulating the patient's active RFID tag using their wireless mobile devices in order to acquire the medical data stored in it.

While the third case which was about locating the nearest available doctor to the patients location, is more concerned about locating doctors than transferring patient's data, so it is not discussed here.

The lower part of figure 5 represents the physical (hardware) encryption layer. This part is divided into two sides. The left side demonstrates the case of a doctor acquiring patient's medical data via a passive RFID tag located in a band around the patient's wrist. The passive RFID tag contains only a very limited amount of information such as the patients name, date of admission to the hospital and above all his/her medical record number (MRN), which will grant access to the medical record containing the acquired medical data and other information regarding the patient's medical condition. This process is implemented in six steps, and involves two pairs of encryption and decryption. The first encryption occurs after the doctor stimulates the RFID passive tag to acquire the patient's MRN, so the tag will encrypt and reply back the MRN to the doctors PDA for example. Then the doctor will decrypt the MRN and use it to access the patient's medical record from the hospital's server. Finally, the hospital server will encrypt and reply back the medical record, which will be decrypted once received by the doctors' PDA.

The right side of figure 5 represents a similar case but this time using an active RF tag. This process involves only one encryption and decryption. The encryption happens after the doctor stimulates the active RFID tag using his PDA which has an in-equipped RFID transceiver, so the tag replies with the medical data encrypted. Then the received data is decrypted through the doctors' PDA.

The upper part of figure 5 represents the application encryption layer. Requiring the doctor to enter a pass-phrase to decrypt and then access the stored medical data. So whenever the doctor wants to access patient's medical data, he\she simply enters a certain pass-phrase to grant access to either wireless mobile device or a hospital server depend where the medical data actually resides.

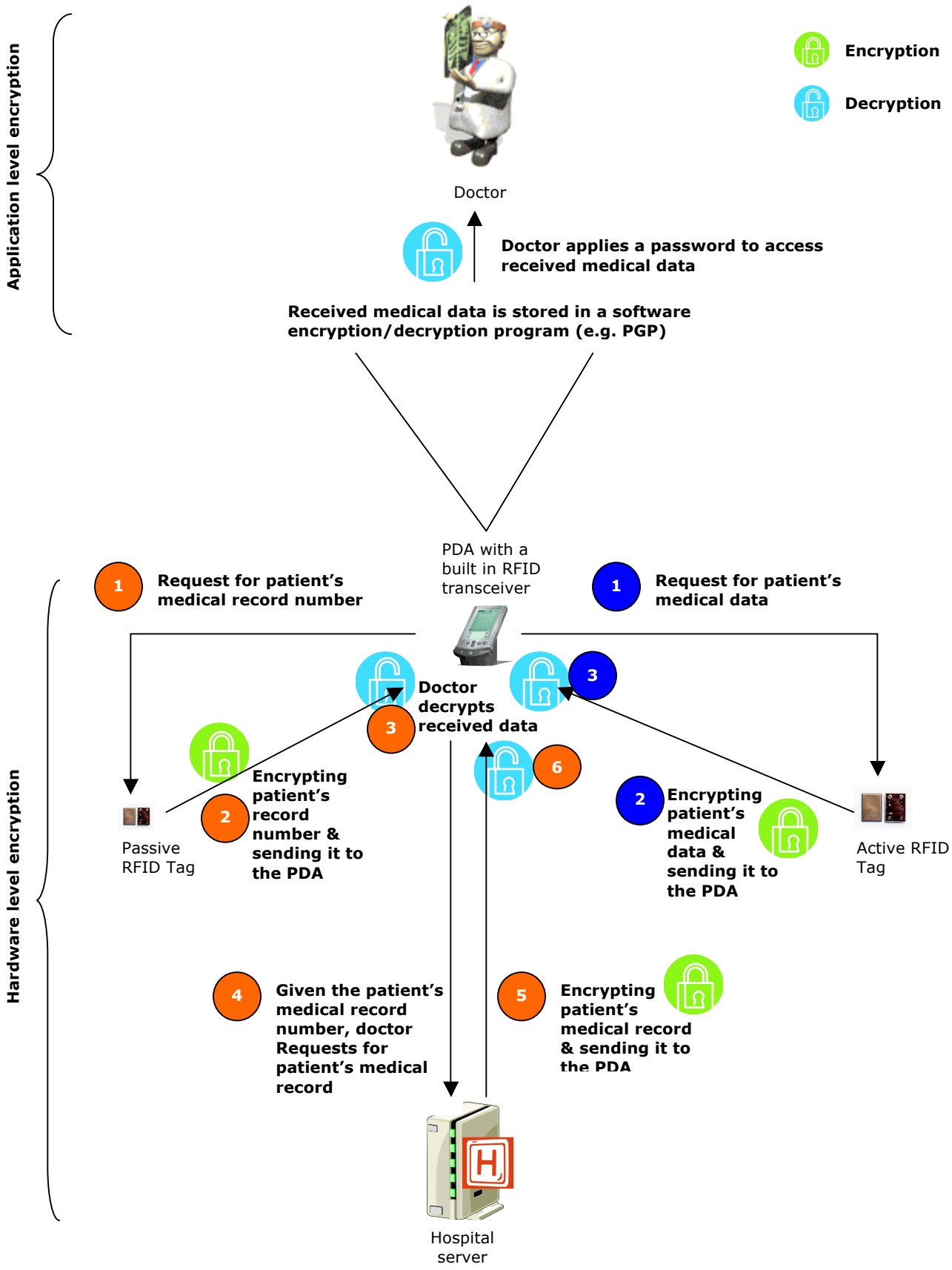


Figure 5: Patient's medical data Encryption framework

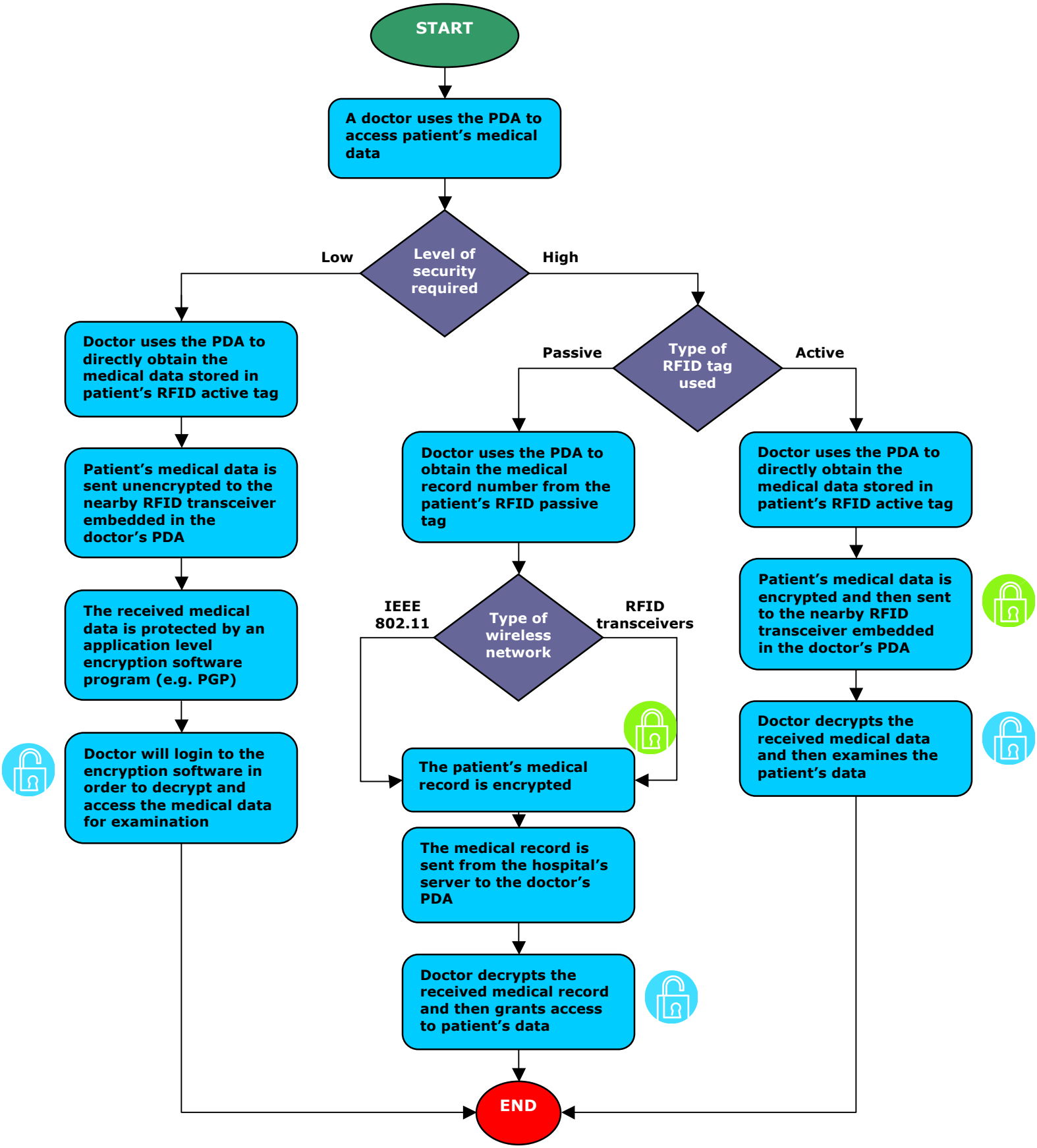


Figure 6: Choosing level of security for the wirelessly-transmitted medical data

Choosing level of security for the wirelessly-transmitted medical data

Securing medial data seems to be uncomplicated, yet the main danger of compromising such data comes from the people managing it, e.g. doctors, nurses and other medical staff. For that, we have seen even though the transmitted medical data is initially encrypted from the source, doctors have to run application level encryption on their wireless mobile devices in order to protect this important data if the devices gets lost, left behind, robbed, etc. Nevertheless, there is a compromise. Increasing security through using multiple layers, and increasing length of encryption keys decreases the encryption\decryption speed and causes unwanted time delays, whether we were using application or hardware level of encryption. As a result, this could delay medical data sent to doctors or on-line monitoring units.

Above, figure 6 represents the case of high and low level of security in a flowchart applied to the previously discussed two cases in the last report.

At the end of this section, we conclude that there are two possible levels of encryption, software level (application layer) or hardware level (physical layer) depending on the level of security required. Both physical (hardware) layer and application layer encryption is needed in maintaining collected medical data on hospital servers and doctors' wireless mobile devices.

Encrypting medical data makes the process of data transmission slower while sending data unencrypted is faster. We have to have a compromise between speed and security. For our case, medical data has to be sent as fast as possible to medical staff, yet the security issue has the priority.

Conclusion

Managing patients' data wirelessly (paperless) can prevent errors, enforce standards, make staff more efficient, simplify record keeping and improve patient care. In this research report, both passive and active RFID tags were used in acquiring and storage of medical data, and then linked to the hospitals' server via a wireless network Moreover, three practical applicable RFID cases discussed how the RFID technology can be put in useful use in hospitals, while at the same time maintaining the acquired patients' data security and integrity.

This research in the wireless medical environment introduces some new ideas in conjunction to what is already available in the RFID technology and wireless networks. Linking both technologies with each other to achieve the research main goal, delivering patients medical data as fast and secure as possible, to pave the way for future paperless hospitals.

References

[1] Current directions Inc (2002). *Introduction to Radio Frequency Identification*. Retrieved August 27, 2003, from Current Directions Inc. website at: http://www.currentdirections.com/facts/introduction-to-radio-frequency-identification.html

Providing a full definition of Radio frequency Identification (RFID) and how this technology differs from bar coding and other available technologies that server a similar role.

[2] The Association of Automatic Identification and Data Capture Technology (2003). *RFID Basics*. Retrieved August 27, 2003, from AIM's website at: http://www.aimglobal.org/technologies/rfid/what_is_rfid.htm

Describing the main components of a RFID system and how we can differentiate between active and passive RFID transponders (tags). Also, explains what RFID transceivers and transponders programmers are.

[3] Marsh, Mike (2002). *Range versus power and frequency for passive electric coupled tags*. Retrieved August 27, 2003, from Transponder News Web site at: http://www.rapidttp.co.za/transponder/index.html

Gives some explanation on frequency ranges that RFID systems operate in.

[4] RFID Australia (2003). *Why use RFID*. Retrieved August 27, 2003, from RFID Australia's Web site at: http://www.rfid-australia.com/files/htm/rfid%20brochure/page4.html

List some important features of transceivers.

[5] CopyTag Ltd (2002). Applications and Solutions: Laptop tracking. Retrieved September 10, 2003, from CopyTag Web site at: http://www.copytag.com/2001/index.html

This Web site provides some pictures of RFID transponders (tags) and transceivers. Also it explains some industrial applications of RFID.