Ατομική Διπλωματική Εργασία

# Security in e-Health: Information classification mapping into security technologies

Ιλιάνα Σταύρου

**ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ**

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Ιούνιος 2006

**ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ**
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

# Security in e-Health: Information classification mapping into security technologies

Ιλιάνα Σταύρου

Επιβλέπων Καθηγητής
Αντρέας Πιτσιλλίδης

Η Ατομική αυτή Διπλωματική Εργασία υποβλήθηκε προς μερική εκπλήρωση των απαιτήσεων απόκτησης του πτυχίου μάστερ Πληροφορικής του Τμήματος Πληροφορικής του Πανεπιστημίου Κύπρου

Ιούνιος 2006

# Acknowledgment

First of all, I would like to express my sincere gratitude to my supervisor, Professor Andrea Pitsillide, for his constant support all these years and for giving me the opportunity to participate in several interesting research projects and attend various international conferences. His help was valuable to finish this thesis work. Also, I would like to thank my parents for their support.

I dedicate this work to Dimitris, for his patience and understanding during the past years. This work would not be made possible without his constant support and encouragement.

# Executive Summary

This research work addresses security-related issues in the electronic and mobile healthcare environments and proposes an appropriate security framework. The proposed framework will identify the necessary security technologies and measures needed to achieve and maintain the security of people, data and infrastructure of the healthcare environment. The study is made in the context of DITIS, a homecare telemedicine application.

The framework uses the OCTAVE risk evaluation methodology to identify the risks and areas of concern that address security challenges that should be taken into consideration when implementing security. The security technologies and procedures proposed in the framework are categorized based on the security objective they serve i.e. confidentiality, integrity, availability, legal conformance. By categorizing technologies based on security objectives we aim in helping people identify the technology they need to implement, based on what they want to protect.

The framework is extended to define a security-level information classification scheme that categorizes information based on its sensitivity (public, internal-use only, confidential, highly confidential). The classification is then associated with the appropriate security technologies that should be considered under each classification level. By associating security technologies with the information classification, the framework aims in balancing the trade-off between security complexity and performance of the system; it will provide guidelines for implementing the necessary measures and technologies, without complicating the operation of the system or saturating its performance with unnecessary functionality.

Finally, an appropriate evaluation is applied on the proposed framework, as well as on DITIS which currently implements some aspects of the framework. Evaluation is essential to assess if the system's security capabilities and procedures represent the security needs and requirements of the users that rely on the system to perform their job well. However, since it is not feasible to conduct a complete system-technical

evaluation as DITIS has not reached its final operational state and security is still an on-going activity, ISO/ IEC 17799 standard entitled *Information technology - Security techniques - Code of practice for information security management* has been selected to evaluate the proposed security framework. The standard provides best practice recommendations on information security management for use by those who are responsible for initiating, implementing or maintaining information security management systems; in general, it deals with the examination of non-technical issues related to personnel, procedural, physical security and security management. Therefore, it could be useful as a high-level evaluation of the proposed security framework, assessing the completeness of the framework against well-known practices. The result of the evaluation is expected to show if the proposed security framework implements adequate techniques and procedures providing the needed protection in the healthcare environment and identify the areas that need to address additional security measures.

# Table of Contents

# Chapter 1

## Introduction



### 1.1 Introduction

Healthcare is associated with mission critical services that are connected with the well being of life. The recent technology and communication advances evolved the healthcare sector in a way that changed the traditional delivery of the healthcare services. Healthcare organizations worldwide benefit from the adoption and usage of electronic and mobile healthcare applications improving the access to medical information and the communication among the medical professionals, thus contributing to the quality of the provided care services.

Electronic and mobile healthcare applications are essential for providing information such as Electronic Patient Records at the point of care, especially for meeting the needs of patients located away from a fully equipped hospital, and supporting the collaboration of healthcare professionals. Due to the critical nature of the healthcare environment and the sensitivity of the information involved, both the e-healthcare and m-healthcare services must be provided in a well secured and protected framework.

The healthcare environment raises a number of considerations; privacy, confidentiality, integrity, legal and ethical considerations affect the intersection of technology and healthcare. Security becomes even more critical with the adoption of m-healthcare

systems, an environment rich with portable digital devices; physical threats, misplacement of devices, insecure wireless/ mobile links and compromization of sensitive data stored on wireless/ mobile devices are some of the challenges that need to be addressed.

Although a number of e-healthcare and m-healthcare applications exist today with some form of security, the security challenges raised in this kind of environment, and the required security technologies, are not adequately addressed. Before moving into the implementation of various security solutions, it is of great importance to research and understand these security challenges and related security issues in order to develop a strong and robust security strategy.

This research work is focused on investigating security-related issues in the electronic and mobile healthcare environments and proposing an appropriate security framework that will identify the necessary security technologies and measures needed to achieve and maintain the security of people, data and infrastructure of the healthcare environment. The study is made in the context of DITIS, a homecare telemedicine application.

## 1.2 Thesis objectives

Electronic and Mobile Healthcare (e-Healthcare, m-Healthcare) applications process sensitive information that requires retaining its integrity and confidentiality at all times in order for the healthcare professionals to provide improved quality of care with the support of Information Technologies. The information stored and processed by these applications, like other important assets, has value to an organization and consequently needs to be suitably protected. Although most of the healthcare applications have implemented some kind of security, none is concerned with the security challenges raised in this environment. Usually, all people understand the significance of having a secure healthcare application but do not really investigate the reasons of such a need; instead they move quickly into implementation of various security techniques. However, it is significant to identify the fundamental need of security and define areas of concern that are vulnerable and need extra attention. By doing so, these areas will be taken into consideration when designing the security strategy of the organization that should include the appropriate measures to address the security issues involved in each area of concern.

Once the areas of concern are identified, a suitable security framework will be proposed and analyzed, including all the appropriate security technologies and measures that are needed to safeguard the assets of the organization that operates the healthcare application. The security technologies and measures will be further categorized based on the security objective they serve (i.e. integrity, authentication, confidentiality, availability) in order to emphasize their role in the information security and for people to know what they will protect when implementing a specific technology.

Finally, the proposed security framework will be extended by defining a security-level information classification scheme that categorizes information based on its sensitivity (public, internal-use only, confidential, highly confidential). The classification is then associated with the appropriate security technologies that should be considered under each classification level. By associating security technologies with the information classification, the framework aims in balancing the trade-off between security

complexity and performance of the system; it will provide guidelines for implementing the necessary measures and technologies, without complicating the operation of the system or saturating its performance with unnecessary functionality.

### 1.3 Thesis outline

Chapter 1 introduces the reader into the study and sets thesis objectives.

Chapter 2 defines the electronic and mobile healthcare environments, discusses related work, analyzes the security challenges that are raised and discusses the European legislative efforts towards healthcare security.

Chapter 3 presents DITIS system and its environment and proposes a security healthcare framework. The framework:

- Uses the OCTAVE risk evaluation methodology to identify the risks and areas of concern that address security challenges that should be taken into consideration when implementing security
- Defines and categorizes security technologies based on the security objective they serve
- Proposes a security-level information classification scheme that categorizes information based on its sensitivity (public, internal-use only, confidential, highly confidential) and it then associates it with the appropriate security technologies that should be considered under each classification level

Chapter 4 assess the completeness of the proposed security framework based on ISO/ IEC 17799 standard entitled *Information technology - Security techniques - Code of practice for information security management.*

Chapter 5 constitutes conclusions and future work.

Chapter 6 lists the publications stemming from the thesis.

# Chapter 2

## Security in Healthcare



### 2.1 Healthcare environment

Healthcare services are provided using appropriate electronic and mobile applications that aid the medical professionals in their every day work to provide high-quality care services. These applications are used to access and process the Electronic Patient Records, independently of the medical professionals' or the patients' physical location. An appropriate infrastructure exists in order to support these healthcare applications, and could include personal computers, mobile and wireless devices, file and application servers, databases and fixed, mobile or/ and wireless networks. Usually, the communication between the device and the infrastructure is established using public networks, such as the Internet.

Eysenbach defines e-healthcare as follows:

"*E-health is an emerging field in the intersection of medical informatics, public health and business, referring to health services and information delivered or enhanced through the Internet and related technologies. In a broader sense, the term characterizes not only a technical development, but also a state-of-mind, a way of thinking, an attitude, and a commitment for networked, global thinking, to improve*

*healthcare locally, regionally, and worldwide by using information and communication technology."* [1]

e-Healthcare solutions [2] include products, systems and services that go beyond simply Internet-based applications. They include tools for health professionals as well as personalized health systems for patients and citizens. Examples include health information networks, sensor and body area healthcare networks, electronic health records, telemedicine and home care services, personal wearable and portable communicable systems, health portals, and many other information and communication technology-based tools assisting prevention, diagnosis, treatment, health monitoring, and lifestyle management.

Although the development and usage of e-healthcare applications [16] changed the way the healthcare sector worked, the introduction of mobile healthcare systems [27] changed the healthcare environment even more and gave it a whole new meaning. The association of mobility in the healthcare environment is a powerful combination that gives the ability to doctors and medical staff to deliver high-quality services to patient located away from a fully equipped hospital. m-Healthcare [3,4] has been described as "the application of mobile computing technologies to provide mobile access to healthcare information systems." m-Healthcare technologies enable access to important and useful information systems at the point of care, from remote locations, or from virtually any place within the healthcare facility using appropriate mobile devices such as pocket PCs, handheld PCs, mobile phones, tablet PCs etc; these devices communicate with a centralized information system to exchange data and provide services to medical professionals.

Due to the critical nature of the healthcare environment, the operation of the appropriate healthcare applications must meet certain requirements [5,6] associated with the protection of medical records, systems and people involved; security becomes even more critical with the adoption of m-healthcare applications. Realizing the security issues involved is a complex and long-term process since healthcare systems are immensely complicated, both in terms of organization and technologies. All efforts should be concentrated on designing a comprehensive security strategy that will address

security issues and provide appropriate solutions to overcome security problems and risks.

## 2.2 Related work

There are a number of commercial projects that provide m-healthcare solutions, especially those that deal with Electronic Patient's Records (EPR). However, none of them considers security as a whole, implementing a comprehensive security solution. Most commercial applications for EPR have been built upon the concept of using PDA's as micro-computers running the healthcare software, and connecting to the central database over a wireless LAN connection.

*Patient Tracker* [74] by HandHeldMed is a widely deployed patient charting application which allows mobile access to patient records and demographics among other reports. It uses simple password protection to protect patient records, and allows simple IR-based peer-to-peer transmission between *Patient Tracker* users. This ability to transmit records without being accountable to a central administration controlled security policy is an inherent flaw which can compromise the confidentiality of patient records.

*Wireless MediCenter* [75] provides a highly efficient solution tailored for portable devices such as PDA's and tablet PC's. It is described by its creators as being "a wireless, paperless electronic medical record (EMR) system." It uses read-write protection for access to the database where the EPR's are stored, and can deliver them over a secure LAN or through high-speed wireless connections, as used by portable devices. It is a comprehensive solution to all doctor and patient needs and provides different portals for the patients to review their information. However, it does not use any notions of trust or digital credentials such as digital certificates which can make the entire application more secure, and also ease the workflow in the environment.

The *m-care* [76] project aims at providing secure access to patient records and other data using a WAP based architecture in conjunction with a WAP-based mobile phone. It uses Wireless Transaction Layer Security (WTLS) to provide network security and personal PIN numbers to provide access to the system. A Microsoft SQL Server holds static information about users and their access rights to the EPR database, and a simple firewall software is used on the server to restrict connections to the service from the

WAP gateway. The use of PIN codes and static access control lists is not sufficient to deal with the accesses needed in a complex healthcare environment such as a hospital, though it may suffice for single individuals out in the field who can only access WAP services and cannot connect to the central database using a more secure wireless technology.

Other custom solutions such as *PatientKeeper* [77] and *PocketMD* [78] attempt similar methods to the above in order to provide EPR's on-the-go but have identical shortcomings to the other applications discussed here.

### 2.3 Security challenges

Healthcare systems are comprised of 4 components:

- People such as healthcare professionals (including administrative staff) that use the system, developers that build the system, or patients
- Infrastructure that involves equipment and networks
- Electronic health records that are the central component of a healthcare system and which allow the sharing of medical information between care providers and patients
- Tools to support healthcare professionals, as for example collaborative tools, calendars, demographics etc

All the above components face a number of security challenges [7,14,17,18,24,25,27, 51,68], including:

- *User authentication*. Sensitive information such as the medical records must be accessed and processed only by those with a "need to know" basis. Otherwise, unauthorized people could reveal confidential information and cause problems to the patients and their reputation.
- *Data integrity*. Medical professionals are depended on the accuracy of the medical data to provide reliable services and treat patients. Otherwise, human life may be at danger. Information should be protected by unauthorized alterations.
- *Network security*. Healthcare systems exchange sensitive information over public networks such as the internet. It is crucial to avoid interception of information over the network since this could lead to modification or even disclosure of medical information.
- *Availability*. Healthcare incidents could be caused any time during the day. Thus, the medical professionals need to be able to access the medical data of the patient to provide him the appropriate treatment. This means that the systems and data must be available on a 24/7 basis.

- *Accuracy of healthcare data*. By introducing a paperless healthcare system, new challenges are raised opposed to the traditional paper system, one of which is the accuracy of the healthcare data. The human factor is responsible for entering healthcare data of a patient in the system and (unintentional) mistakes could happen when providing such data as drug descriptions. If this happens, then the patient is in danger due to erroneous data that could be used for his treatment.
- *Quality of Service*. Medical professionals are interested for providing the best care at the minimum time. They need to quickly access the healthcare system and perform their job easily and efficiently. This requirement many times is prohibited due to the complexity of the security technologies implemented. The challenge here is to balance efficiency with the trade-off of security.
- *Physical security of data and systems*. Although communication is made electronically, most of the times we overlook the obvious problems. Physical security of systems and data involves issues relating to the physical access to hardware systems and data, theft prevention, backup and disaster recovery, and the security of sensitive devices such as mobile terminals.
- *Legal and liability issues*. The storage and processing of healthcare information must be performed according to appropriate European and national legislation since it is vital for both the patients and the care providers to be legally covered; the former have the right for privacy while the latter must be protected in cases they performed their job as expected. Additional challenges are raised concerning liability issues. Healthcare systems must be in position to identify professionals that made a change on the data or took an action and take responsibility of this, if required.
- *Ethics*. Care providers must be governed by professionalism and operate within the medical confidentiality oath. They must be aware and acknowledge the importance of safeguarding medical data in order to provide quality healthcare services.
- *Education of users*. Both the patients and the medical professionals must be informed about their rights and educated appropriately. Patients must get informed about the legislation that protects their right to privacy while medical professionals must be educated about the correct and safe usage of the system

as well for the appropriate procedures they must follow. Education is vital in order to build trust and confidence among people that either rely on the system to provide their services or receive services based on data stored on it.

- *Mobility*. Special security considerations and challenges are raised when mobility is introduced in the healthcare environment; presence of foreign users, very large number of users and resources, difficulty in maintaining central control, and communication over insecure wireless links. Furthermore, due to their small size, handheld devices may be misplaced, left unattended, or stolen; user authentication may be disabled, a common default mode, revealing the contents of the device to anyone who possesses it; even if user authentication is enabled, the authentication mechanism may be weak or easily circumvented; the ease with which handheld devices can be interconnected wirelessly, combined with weak or no authentication of the parties involved, provides new avenues for the introduction of viruses or other types of malicious code, and also other forms of attack such as a man-in-the-middle attack. In addition, limitations of mobile devices (limited battery life, computational power) often affect the adoption of security technologies.

## 2.4 European efforts

Use of information technology offers great potential for patients, professionals and for health systems overall. Health-related information is already one of the most searched-for topics on the internet, as citizens look to be better informed about their health and decisions affecting it. Data privacy and security in e-healthcare have a European dimension [8, 15]. The Commission is taking forward actions [9] to promote secure e-healthcare as part of the European e-health action plan.

The confidentiality and protection of patient data is governed by the general European Union rules of data protection and privacy of electronic communications.

The Data Protection Directive 95/46/EC [10] addresses the protection of individuals with regard to the processing of personal data and on the free movement of such data. The objective of this Directive is to harmonize data protection legislation in the Member States, in order to facilitate the free movement of personal data within the Union while protecting the fundamental rights and freedoms of natural persons. The Directive contains a general prohibition on processing sensitive data, including data concerning health, but with a limited number of exceptions. In particular, the general prohibition on processing sensitive data may be lifted if the subject of the data gives their explicit consent, provided that the laws of the Member State concerned allow individuals to give such consent. Health data may also be processed in situations where this is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health care services, and where those data are processed by a health professional who is subject to the obligation of medical confidentiality or by another person also subject to an equivalent obligation of secrecy. Although the directive provides a framework for handling personal data and health data in cross-border care, awareness of these provisions may not be sufficient in the health sector. If they are not applied, this may mean that the privacy of citizens is not properly respected – or conversely, that relevant information for their care does not follow patients when they seek care elsewhere within the Union. The Commission will work with the Member States and with the national data protection authorities to raise awareness of

these provisions as they apply to healthcare and to address any outstanding issues if needed.

The Directive 2002/58/EC on Privacy and Electronic Communications [11] harmonizes the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the electronic communication sector, regardless of the technologies used and to ensure the free movement of such data and of electronic communication equipment and services in the Community. The provider of a publicly available e-healthcare service must take appropriate technical and organizational measures to safeguard security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security. Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented. In case of a particular risk of a breach of the security of the network, the provider of the e-healthcare service must inform the subscribers concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved.

The Electronic Commerce Directive 99/93/EC [12] which creates a legal framework for the provision of information society services, also applies to the provision of online health services. The Directive, principally by virtue of its internal market clause, contributes to the legal certainty and clarity needed for the provision of online information society services throughout the entire Community. In particular, its provisions on information and transparency requirements, commercial communications, the liability of intermediary service providers, and the basic principles it establishes regarding electronic contracts, provide for high standards in the provision of online services in all Member States, thus also increasing consumer confidence.

The Electronic Signatures Directive 93/93/EC [13] defines that electronic signatures have the legal equality with hand-written signatures and creates the legal and technical framework that verifies the uniqueness and origin of the electronic signatures. The authenticity and integrity of the electronic documents in the healthcare environment are

of great importance. A signature is the expression of approval of the author with the content of a writing to which he consents and accepts the legal consequences. In order to attach legal effect to a signature one has to ascertain its origin. The signature is unique. Indeed the identification of the signature guarantees the non-repudiation of the will of the person behind the signature. The author of the signature must be the one who is committed. The need to identify a person unambiguously is a most important component of the interoperability of health information systems. The development of the electronic transfer of documents requires the legally acceptance of electronic signature. The electronic signature directive is therefore a necessary tool for the electronic medical prescription. By means of an electronic qualified signature, the medical doctor may electronically send a secure and certified medical prescription to the pharmacist. By means of the electronic signature the patient may also correspond individually and safely with the online pharmacist.

Another important legal issue is liability in the event of problems - such as technical malfunctions of the system, network, or provision of the service itself - that result in serious harm to a patient. While there are currently no specific guidelines or liability rules, as with any emerging or growing area of practice, only the increased use of e-Health applications and the performance of e-Healthcare will make its potential fully visible as well as raising any remaining legal uncertainties.

Further steps might be considered if they could show that even greater legal certainty would reinforce patient confidence in e-Health services. Similar safeguards for qualifications might also be useful. Building trust is a prerequisite to the development of an information society, in e-Health probably more than anywhere else. Citizens prefer services and information tailored to their needs and requirements, while knowing that their right to privacy is protected. The Commission advocates that it will work with the Member States through appropriate Healthcare groups to raise awareness of these provisions and to address any outstanding issues.

# Chapter 3

## Security Framework



### 3.1 Introduction

This chapter investigates security-related issues in the healthcare environment and proposes a security healthcare framework. The study is made in the context of DITIS healthcare application, involving:

- Adoption of the OCTAVE risk evaluation methodology to identify the risks and areas of concern that address security challenges that should be taken into consideration when implementing security
- Definition and categorization of security technologies based on the security objective they serve
- Definition of a security-level information classification scheme that categorizes information based on its sensitivity (public, internal-use only, confidential, highly confidential) and it then associates it with the appropriate security technologies that should be considered under each classification level
- Implementation of the security framework in DITIS

## 3.2 DITIS Case study

The healthcare application and its infrastructure considered for this research are used to drive the security analysis that derives the areas of concern that will be taken into consideration when designing the security strategy. This section defines DITIS environment, its main services and functionality that are considered for the study.

### 3.2.1 Environment

DITIS [19,20] (in Greek it stands for Networked Collaboration for Home healthcare) is an Internet-based Group collaboration system with fixed and GSM/GPRS mobile connectivity.

DITIS was initiated in 1999, supporting the activities of the home healthcare service of the Cyprus Association of Cancer Patients and Friends (PASYKAF). DITIS supports homecare by offering wireless healthcare services for chronic illnesses with emphasis on prevention, assessment and diagnosis. The main service is the dynamic creation, management and co-ordination of *Virtual Collaborative Healthcare Teams* for the continuous treatment of a patient at home, independently of physical location of the team's members, or the patient. For each patient a flexible (dynamic) virtual medical team is provided, made up from visiting homecare nurses, doctors, and other healthcare professionals, responsible for each case that may not be physically located at the same time at a particular patient. The team has easy and timely access to the unified Electronic Medical Record database to retrieve information about a patient i.e. the current medical treatment and modify it as needed, as well as a range of collaboration tools and services. Currently, the main mobile device used within DITIS application is Sony Ericsson P900 mobile phone.

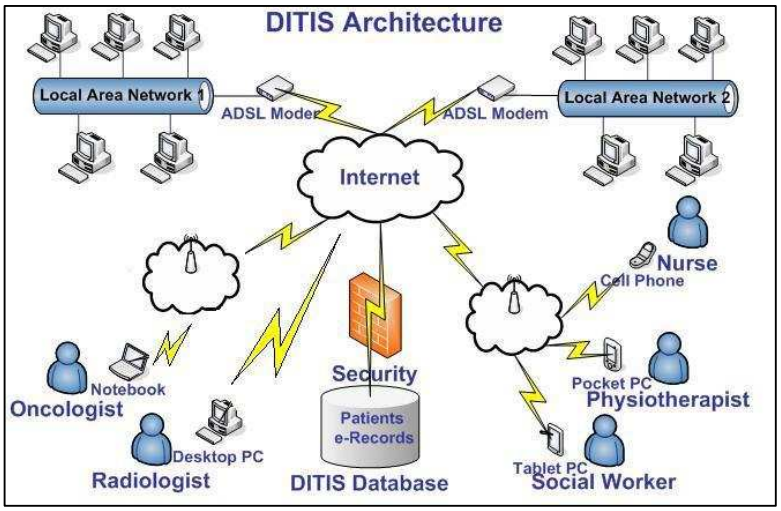


Figure 3.1: DITIS architecture

### 3.2.2 Stakeholders

Currently, DITIS application is used by the following categories of people:

- Healthcare professionals (i.e. oncologists, cardiologists)
- Nurses
- Therapists (i.e. physiotherapists, social workers)
- Secretarial personnel

All people aforementioned are working for the welfare of the patients.

### 3.2.3 Functionality

The main services that are provided through DITIS application are the following:

- Demographics
- Medical history
- Symptoms registry

- Diagnosis
- Treatment
- Medication
- Virtual Team registry
- Statistics
- Appointments

Following is a plausible scenario illustrating aspects of DITIS functionality.

Nurse Mary wakes up early in the morning. After showering and a quick breakfast she connects (with her Mobile Computing Unit, MCU, such as a Smart Phone, Pocket PC etc…) to the central office web server to check in and acquire her day's visit schedule (the nurse does not have to physically check in). Her schedule includes a number of visits. For each patient to visit, Mary downloads on her MCU the needed information, plans her route, and updates the Web server of her schedule.

At first she visits Mr. P., a nice sweet old man who while enjoying the comfort and love of his home he regularly requires (and receives) attention due to the seriousness of his situation. Arriving at his house and examining Mr. P. nurse Mary realizes an extreme change in his condition. She immediately (via GSM/GPRS) connects with the web server and via the MCU's application interface reports the incident. The system records (into the electronic medical record of the patient in the database) the new data, and based on the identified/pre-wired scenario triggers and transmits messages to the other members of the team alerting them and requesting their services.

For each member of the team DITIS extracts from the EMR only the needed (and authorized) parts of the information, prepares it and then forwards to them. That is the MCU device of every team member is receiving not only the data of the triggering incident (i.e., patient P. experiences extreme pain in the lower back) but also relevant patient history. (The virtual team around patient P. has now been set in motion in seconds defying distance and geographical barriers.)

The responsible doctor, Dr. A., studies the information submitted to her and prescribes the health care protocol which nurse Mary and other team members (e.g. a prescribed physiotherapy) should administer. Also a new appointment is scheduled for patient P. with the oncologist. Nurse Mary performs her tasks and Mr. P. returns back to his smiley and happy self; the virtual medical team made the 'miracle'. His family is thanking nurse Mary who is headed to her next appointment. She is checking her schedule when a message comes in informing her that Mrs. D., her next patient, has suffered an extreme crisis and she has been taken to the hospital. Nurse Mary, while sorry for Mrs. D., is headed to the next patient in her list, Mr. X. Nurse Mary examines patient X. and updates the database accordingly. And so the day goes on.

## 3.3 Security analysis

A number of security solutions exist today to protect information, systems and people. However, technology is useful only when used properly; depending on the security needs and requirements present at each situation, appropriate technology must be addressed. In DITIS system, it was a high priority to investigate and address the security issues related to DITIS environment such as privacy, confidentiality, integrity, legal and other security-related considerations. By doing so, possible threats and risks could be addressed and appropriate security solutions could be applied.

This section emphasises the need to identify appropriate security areas of focus [66] based on the nature of the application / environment under consideration and its security needs. The target is to identify vulnerable areas that need special attention before moving into implementation. In this way, the development team will be able to address and implement appropriate security technology providing an enhanced level of protection to each area. After the areas of focus are identified, an appropriate study will be made resulting in a proposed security strategy that will address the areas that are listed within the current study.

Following, the security analysis applied on DITIS is presented in detail.

### 3.3.1 Risk evaluation

It is a common acceptance that most of times people involved in software development place their focus on the implementation of the requirements rather than solving security issues. However, security is not an issue that can be overlooked since security incidents are reported every day, some of which may cause great damage to an organization. Therefore, it is crucial to design a comprehensive security approach in order to face security problems.

The initial step of a strong security approach should be the risk analysis and evaluation process [26]. Risk analysis involves identifying assets that need protection and evaluating possible threats against these assets. Specifically, it is a process that ensures that the security controls of a system are fully commensurate with its risks. The value of performing a risk analysis is that it helps out developers to focus their attention on the possible threats their application and assets are facing by having a better understanding of the environment; after all, before someone can protect something he has to know that it is at risk. Beyond the improved awareness risk analysis may raise, it also helps in improving the basis for decision; based on the risks and security needs the right decisions could be made to adopt appropriate security technology without affecting user and system performance. Furthermore, risk analysis could justify security costs since it helps identifying security mechanisms that are worth the expense.

There are different approaches toward risk analysis, one of which is OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation). OCTAVE [21,22,23] is a risk based strategic assessment and planning technique for security. By using the OCTAVE approach, the organization can make decisions regarding information security countermeasures that preserve the Confidentiality, Integrity and Availability model of critical information-related assets. All aspects of risk (assets, threats, vulnerabilities, and organizational impact) are evaluated and factored into decision making, enabling an organization to match a practice-based protection strategy to its security risks.

The OCTAVE method uses a three-phase approach to examine organizational and technology issues leading to a clear view of the security needs. In phase 1, critical assets are identified and threats against these assets are reported. Phase 2 is an evaluation of the information infrastructure identifying vulnerabilities that can lead to a security incident related with the critical assets. Phase 3 identifies the impact of threats to critical assets, develops criteria to evaluate the risks and finally creates a protection strategy.

As mentioned earlier, DITIS is a telemedicine system used by PA.SY.KA.F, a small-to-medium organization. Since OCTAVE is focused on large-scale organizations, it was appropriately adopted to meet the size and target of the organization. However, the main

context of the model was maintained throughout the case study. Feedback for each phase was gathered through a combination of techniques; questionnaires and interviews were used to gather the healthcare team's considerations towards security issues and protection of medical records, document review such as system documentation (manuals, documented vulnerabilities), similar case studies, legislative documentation, and usage of automated scanning tools were used to evaluate the architecture's components and provide information for designing a strong security strategy.

Following, the phases used to apply the OCTAVE risk model are presented.

#### 3.3.1.1 Identification of assets

The first step of a risk analysis is to identify the assets of the company. The assets can be collected into categories i.e. hardware, software, data, people, documentation. This listing is essential in order to know what we are trying to protect and in what degree.

After evaluating DITIS architecture and operational procedures, critical assets have been identified. With respect to:

- Hardware, personal computers, mobile devices (i.e. tablet pcs, mobile phones, personal digital assistants), web servers and database servers are listed. The healthcare team uses mobile devices and personal computers to access the Electronic Medical Record and retrieve information about a patient, at the time of need. Web and database servers are part of the architecture that support web accessing and storing of medical records, respectively.
- Information, electronically stored medical records are listed as the number one critical asset of the organization. Medical records are accessed by mobile devices to provide quality and efficiency in the provided homecare services. Information asset also includes software coding and documentation.
- Software, the application is listed. The healthcare team depends on the functionality of the application to perform well in their job.

- People, expertise is listed. The development team of DITIS includes professionals working in areas such as database / web / mobile programming, security, analysis and design and system modeling. Since up to two persons are involved in each area, absence of a member of the team for any reason (i.e. quit, vacation) could cause huge problems. Furthermore, the healthcare team of DITIS includes a number of healthcare professionals (i.e. oncologists, nurses, physiotherapists), some of which have expertise in using computing systems and some others have minimum computer skills.

Identification of the critical assets of the organization will drive all future actions of risk analysis. Therefore, it is essential to produce a comprehensive listing of all critical assets that could be in danger in the case of a security breach and need to be protected.

#### 3.3.1.2 Identification of threats

The next step of risk analysis, based on the profile of the organization, is to determine the threats [28,29] that may cause damage to the assets of the organization. By identifying the threats a strong level of protection could be applied to defeat any threat that may put the organization at risk.

Based on DITIS profile and taking into consideration the fact that DITIS is a mobile telemedicine application, security goals that must be met are set to:

- Confidentiality. Confidentiality ensures that sensitive information is available only to those who are authorized to access it. Since information is related to sensitive personal information such as medical records, Data Protection Law restrictions should be followed. Furthermore, the network architecture and sensitive configurations must be kept secret from people without the need to know.
- Integrity. Integrity protects systems and information from unexpected modifications. Medical records must be kept accurate and be modified by

authorized personnel. System configurations must be up to date and modified by authorized members of the development team to preserve the stability of the system.

- Availability. Information and systems should be accessible at any requested time. Due to the nature and criticality of the healthcare sector, medical records and systems must be available on a 24/7 basis to nurse patients quickly and effectively at any time needed.
- Authentication & Authorization. A&A are two related concepts. Authentication provides a way to proof identify of a user and authorization determines whether an authenticated user has the credentials to carry out a certain activity. Healthcare and development team members should be assigned special credentials to access the system and information stored on them. Proper security education should be provided to prevent people from exchanging passwords or performing other actions that could endanger the safety of people, information and systems.
- Access control. Access control protects the system and resources against unauthorized usage. Different access control mechanisms should be provided to safeguard different levels of sensitivity. For example first level access control should be implemented for information shared between the healthcare team while second (or more) access controls should be applied for information designated for a group of users i.e. nurses, social workers, physiotherapists.
- Accountability. Actions taken by legitimate users can be tracked down. By doing so, a user is accountable for his actions. Mechanisms should be in place to protect people from been accused for something they did not do. In addition to this, appropriate legislation must be in place to legally cover innocent people.
- Physical security. Since the study is focused on mobile healthcare applications, physical security of the mobile devices is a critical objective that must be achieved in order to protect sensitive information that is stored locally on the devices. Mobile devices can be easily misplaced or lost. Therefore, appropriate techniques must be applied to maintain security even though a mobile device is stolen.

The following table presents the threats found against the critical assets of the company and the security goals identified.

| THREATS | | | | |
|---|---|---|---|---|
| ASSET / SECURITY GOALS | HARDWARE | SOFTWARE | INFORMATION | PEOPLE |
| Confidentiality | -Disclosure of the architecture<br>-Hardware theft | -Stolen, copied<br>-Modified (maliciously or unintentionally) | -Stolen, copied, deleted<br>-Disclosure of medical information<br>-Blackmail | -Dishonesty, blackmail<br>-Lack of security guidelines towards incident response<br>-Unintentionally reveal security information to adversaries |
| Integrity | -Tampered with<br>-Damaged (maliciously or unintentionally) | -Illegal modifications<br>-Malicious programs<br>-System exploitable bugs<br>-Misconfigured software | -Maliciously or accidental modifications<br>-Transmission errors<br>-Malicious programs<br>-Sniffing<br>-Unable to verify integrity of received data | -Dishonesty |
| Availability | -Failed due to technical errors<br>-Denial of service attacks<br>-Malicious programs i.e. viruses, Trojan horses<br>-Physical threats i.e. fire | -Deleted, misplaced<br>-Denial of Service attacks<br>-Malicious programs<br>-Lack of backups | -Deletion of medical records<br>-Misplaced<br>-Denial of Service<br>-Malicious programs | Quit, On vacation |
| Authentication | -Weak authentication procedures<br>-Lack of policy<br>-Social engineering<br>-Eavesdropping<br>-Authentication based on false credentials | -Weak authentication procedures<br>-Lack of policy<br>-Social engineering<br>-Eavesdropping<br>-Authentication based on false credentials | -Weak authentication procedures<br>-Lack of policy<br>-Social engineering<br>-Eavesdropping<br>-Authentication based on false credentials | -Masquerade as legitimate users<br>-Social engineering<br>-Sniffing |
| Access control | -Unauthorized physical access to hardware<br>-Backdoors | -Unauthorized access<br>-Backdoors<br>-Brute force attacks | -All users have the same view of data | -Misconfigured access control |
| Accountability | -Procedures not in place to identify who has in his/her possession a hw device<br>-Appropriate documents not in place i.e. proper usage policy | -Procedures not in place to identify who and when changed code | -Receivers of confidential information may refuse to acknowledge receipt<br>-Communicating parties are not verified as trusted<br>-Medical records used without the consent of the patient | -Receivers of confidential information may refuse to acknowledge receipt<br>-Communicating parties are not verified as trusted<br>-Medical records used without the consent of the patient |

Table 3.1: Identification of Threats

After studying the threats that could endanger the safety of the organization, DITIS team identified potential threat-sources that could initiate a threat. Three categories of threat-source were identified:

- Non-malicious employees. People within the organization who accidentally cause damage to computer systems and information due to lack of security education or negligence.
- Malicious employees. People within the organization who deliberately misuse systems and information i.e. terminated or disgruntled employees.

- Attackers. People who attack computer systems to cause damage i.e. disclosure of information, illegal modifications, exploitation.

These categories will be taken into consideration when designing the security strategy. Appropriate mechanisms should be implemented to act proactively against potential security threats.

Beyond the identification of operational and technological threats, DITIS development team evaluated the components of the infrastructure along the recommendations provided from vendors and run vulnerability evaluation tools against key components. The target was to identify technology vulnerabilities associated with each component that could lead to unauthorized access to the system causing great damage, and apply the necessary measures to prevent it. Listing vulnerabilities of key components is out of the scope of this study since they are related with specific vendor technology that may not be applicable in other situations.

#### 3.3.1.3 Identification of impact

This section defines impact descriptions for threat outcomes (disclosure, modification, loss, destruction, interruption of critical asset). The impact description is a narrative statement that describes how a threat ultimately affects the organization's mission.

- Disclosure: Failure to safeguard privacy would result in loss of credibility of the organization. This will lead to bad publicity. Reputation of patients may be damaged, for example they could loose their job. Patients will not give their consent to store personal information electronically or even they will seek care from another source. Healthcare team will stop using the system and return to paper workflow.
- Modification: Provision of healthcare services may be affected and not delivered correctly since malicious modifications could affect appointments, medical

treatment and productivity. Patients' health could be affected due to improper changes to medical records.

- Loss / Destruction: Information is impossible to reconstruct or it can be reconstructed partially or totally. Trying to verify and reenter what was lost between the last backup and the present would consume a lot of time and resources.
- Interruption: The healthcare team cannot deliver its services effectively. The system and information stored on them are not available at a requested time.

Each threat is related to a potential impact on the critical assets of the company. The scope of this step is create threat profiles by establishing a link among assets, threats, and impacts, providing a basis on which the risks can be analyzed and calculated.

The following figure shows the threat profile associated with medical records identified by DITIS team. As the figure shows, medical records are endangered by malicious code that could cause modifications to information, disclose sensitive data and interrupt the services provided by the application; telecommunication problems could lead to extended interruption of provided services if the problem is not recovered immediately; weak authentication procedures could allow users to guess passwords of legitimate users which they then use to gain unauthorized access to the system and destroy, modify or disclosure information for their own illegal purposes.

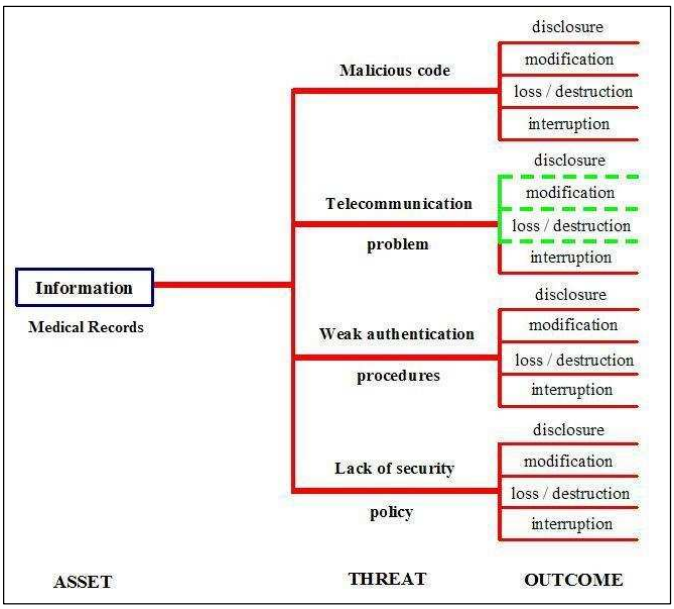


Figure 3.2: Identification of impact

#### 3.3.1.4 Create risk evaluation criteria

Evaluation criteria are measures against which the impacts identified previously are evaluated. The evaluation criteria define the organization's tolerance for risk for a certain impact. Before conducting an evaluation, a set of impact areas are identified which they constitute critical areas that if affected could cause great damage to the organization and people involved. DITIS team identified the following impact areas based on the nature and objectives of the organization:

- Organization's Reputation. Above all, if the patients do not trust the organization for providing effective and quality of services, they will move to other organizations. This could lead to the closing down of the organization.
- Patient's confidence. If the patients do not place their trust to the system anymore due to a severe security breach and do not consent in storing their sensitive medical information electronically, then the system gets ineffective and quality of provided services is degraded.
- Healthcare team's confidence. The system success depends on the full adoption and usage by the members of the healthcare team. If they fear technology or they are not convinced that medical records are well protected, then they will not use the system but rather they will provide services based on the traditional paper workflow.
- Productivity. If a security breach is successful, this could decrease productivity. The healthcare team may need to spend more effort and time to provide services which normally need fewer resources to be delivered successfully.
- Life continuity. Number one consideration of the healthcare team is the health of its patients. Any security breach that could lead to loss of life must be prevented. The healthcare team must be reassuranced that this would be the case.
- Legal Penalties. A number of laws exist today to protect the sensitive information of citizens such as medical records and religious beliefs from disclosure. The organization and its members must act accordingly to the guidelines of the law, otherwise they could be found responsible of causing damage and face penalties defined by the law.

The following table defines a three-scale measurement (low, medium and high), each having its own evaluation criteria against each area of impact.

| EVALUATION CRITERIA | | | |
|---|---|---|---|
| **Area of Impact** | **Low** | **Medium** | **High** |
| Organization's Reputation | • Reputation minimally affected; little or no effort or expense required to recover | • Reputation damaged; some effort and expense required to recover | • Reputation irrevocably destroyed or damaged |
| Patient's confidence | • Patient's confidence is minimally affected<br>• Considerations on behalf of the patients about storing their personal information electronically<br>• Less than 5% of customers seek care from other sources | • A portion of patients (up to 30%) do not consent in storing their personal information electronically<br>• 10 to 30 % of patients seek care from other sources | • More than 40% of patients do not consent in storing their personal information electronically<br>• More than 40% of patients seek healthcare from other sources |
| Healthcare team's confidence | • The healthcare team expresses its considerations towards security of medical records | • The healthcare team is partially using the system along the traditional paper workflow | • The healthcare team is not willing to use the system any more to provide their services |
| Productivity | • Healthcare team work hours are increased by less than 5% for 1 to 5 days | • Healthcare team work hours are increased between 5% to 10% for 5 to 10 days | • Healthcare team work hours are increased by more than 10% for more than 10 days |
| Life continuity | • No loss or significant threat to patients' lives | • Patients' lives are threatened but they will recover after receiving medical treatment | • Loss of patients' lives |
| Legal Penalties | • Non public violation of data protection law – disclosure to healthcare personnel with a need to know bound by the medical confidentiality | • Disclosure to healthcare personnel without the need to know<br>• The organization is legally prosecuted. Some form of legal action is taken against the organization | • Disclosure to anyone who violates the data protection law and reveals sensitive medical information<br>• The organization is legally prosecuted (negligence, breaking the law etc). Legal actions are taken against the organization |

Table 3.3: Risk Evaluation Criteria

#### 3.3.1.5 Calculation of risk-impact

Finally, the risk analysis ends up by calculating the magnitude of impact towards the evaluation criteria by assigning the impact description a value: high, medium, or low.

The following table shows the magnitude of damage / loss that could result due to a number of threats launched against medical records maintained by the system. By defining the magnitude of impact, the organization can identify the main threats and prioritize them in a way to help design and implement the appropriate security

technologies overcoming possible security breaches. For example, interruption of provided services due to telecommunication problems has a low impact on the organization because it cannot endanger the information included in the medical records. However, if the impact was defined on the quality of the provided healthcare service it would have a medium to high affect depended on the time required to recover the connection with the system; many times, the quality of the healthcare services depends on how quickly a user can access the system and retrieve the medical record of a patient, especially when there is a healthcare incident.

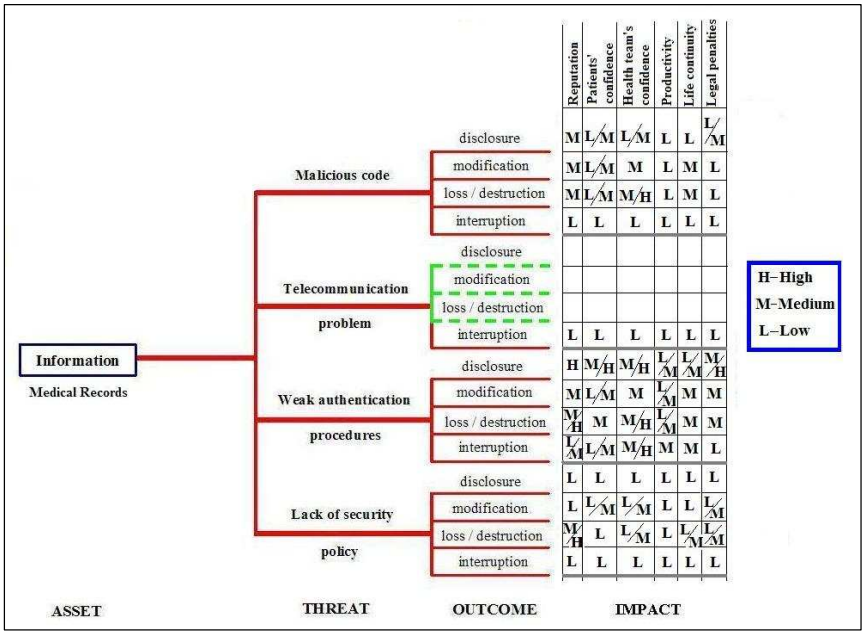


Figure 3.4: Calculation of risk - impact

### 3.3.2 Areas of concern

As mentioned earlier, the risk analysis methodology was applied to determine areas that are vulnerable and need extra attention to prevent security violations. After studying the results of the risk analysis, the following areas were identified, and which

must be taken into consideration when designing the security strategy of the organization:

- Security awareness. The study revealed lack of adoption of security practices such as using strong passwords and applying antivirus on downloaded documents. Many times ignorance could cause the same damage as an intentional illegal action. Before trying to secure the organization from outsiders, appropriate measures should be taken to safeguard assets from security unaware employees.
- Access control. The healthcare team of DITIS includes a number of professionals; oncologists who are based in the oncology center, treating doctors who are usually located in the community, homecare nurses who visit the patient regularly at home, and a number of other professionals called in as the demand arises, typically physiotherapists, psychologists, and social workers. Each group of users handles different data about a patient related to his / her job function. There is the need to assign different permissions to each group of users providing an appropriate view of the Electronic Medical Record. In addition to this, access control mechanisms should be strong enough to prevent an attacker who stole a mobile device to access information stored on it.
- Ethics & Legislation. The healthcare team is bound by the medical confidentiality and its first priority is to respect the patient's right for privacy as identified by the law. However, not all people involved in the organization are bound by the medical confidentiality i.e. a secretary. Appropriate mechanisms should be implemented to prevent people outside the medical confidentiality to access confidential information. Furthermore, nurses fear taking responsibility for an action that was taken by someone else, for example change the medical treatment of a patient. However, although the nurses are responsible for the provided treatment in accordance to the prescribed protocol, they are not responsible for its selection. Further mechanisms should be in place to track users' action and prevent situations like the one described. Generally, if anyone (including the healthcare members) is found compromising confidentiality must face appropriate penalties set by the organization and the law.

- Transparency. The patients have the right to be informed when their personal data is stored and processed electronically as defined by the law. The healthcare team is obligated to inform the patients that they use their personal information to provide their services and also ensure that the patient can access his information and correct inaccurate data. In addition, the healthcare team feels that it is important to have the written consent of the patients to store and process their personal data so that they are legally covered in a lawsuit.
- Quality of services. The scope of developing any e-healthcare application is to provide quality of services. Considerations are raised towards usability and a number of security requirements. Since mobile devices are constrained by a limited screen, available security services must be easy to use and designed having in mind usability concepts. Regarding the security requirements: loss of availability can cause severe damage; nurses fear situations where a patient may need immediately care and they could not access his medical record in order to find his medical treatment and act accordingly. Loss of integrity is unacceptable since it would affect the provided care services. Mechanisms to safeguard that information is traveling from one end to the other without being intercepted and modified in the process should be implemented. Furthermore, quality of healthcare services is dependant on an effective security management. A structured administration is needed to immediately respond to problems. The team must feel the presence of a person that will help them with the system if they have a problem. Placing confidence to the system is not an easy task to do as some members of the team have until recently been working with the traditional paper workflow. Therefore, the need of having a structured administration is a must.

### 3.4 Security framework

This section presents a proposed security framework for healthcare applications, initiated by OCTAVE risk assessment methodology. The areas of concern identified previously, leads to the design and implementation of a multi-layer security architecture to provide strong protection to the system, data and people involved. The architecture consists of the necessary security mechanisms and technology that are needed to safeguard the electronic healthcare environment. Each security mechanism that is proposed is briefly described. The security framework is implemented in DITIS; some of the technologies are still under development in DITIS environment.

The objective of the proposed security framework is to establish appropriate security procedures and technologies [8,14,30-38,44,45,53,65,68,69,73] to protect sensitive information and systems from the following:

- Interception of data transmission
- Unauthorized access
- Network attacks
- Lost devices

These issues are found during the communication between:

- *The healthcare service provider and the device*. This is the initial point in the process of a transaction. This stage implicitly assumes that the person originating a transaction is the device owner and is an authorized user. Unfortunately, this leads to an uncomfortable assumption that the possessor of the device is indeed an authorized healthcare user and the owner of the device. To ensure end-to-end security, a number of issues must be resolved: can a transaction be prevented if an unauthorized person tries to masquerade as a legitimate user and engages in a transaction? If an unauthorized transaction occurs, is the provider who has the true ownership of the device liable? Also, what is the liability of the organization if an unauthorized person successfully completes a healthcare transaction leading

to undesirable consequences for one or more patients? Conversely, if the mobile device is stolen, can a transaction be prevented?

- *The device and the ISP operator*. This stage of a transaction occurs over the open air when using mobile devices. Typically, the user's directive is transmitted from his mobile device to a base station. Since the data transmission is wireless, there is a possibility of intercepting the radio transmission. If an adversary can intercept a transmission, not only there is loss of confidentiality but also other potential consequences. For example, the adversary may be able to gain access to confidential information about a patient and maliciously change medical directive leading to severe damage or even to loss of life.

The proposed security mechanisms included in the framework are categorized based on the security requirements they fulfil. This categorization is deemed necessary for having a clear view of what each technology is used for and what it can protect. In this way, a mechanism is chosen to supplement the others in an attempt to create a comprehensive and strong security strategy.

### 3.4.1 Authentication

Authentication is the process of recognizing and verifying valid users, processes or devices, and ensures that only legitimate users may access systems and information stored on them. A combination of authentication mechanisms should be implemented according to the security level defined.

There are three main ways to authenticate an identity:

1. Something you know, like a password or pass phrase
2. Something you have, like a token
3. Something you are, a measurable trait

These are often referred to as the three pillars of authentication. They can be used separately or combined for even stronger authentication.

#### 3.4.1.1 PIN / Password

Mobile device users must be able to authenticate themselves to the mobile device by providing a Personal Identification Number - PIN (i.e. for mobile phones), a password (i.e. for PDAs), or both. Passwords have been successfully providing security for computer systems for a long time. They are integrated into many operating systems, and users and system administrators are familiar with them.

Attention is needed when choosing weak PINs or passwords since they could easily be compromised and give access to an adversary that would masquerade as a legitimate user. At the most basic level, organizations should require the selection of strong passwords that would be difficult to guess. Ofcourse, complex passwords introduce new problems; if they are hard to remember people would be tempted to write them down with the risk of revealing the password to anyone.

#### 3.4.1.2 Public Key Infrastructure (PKI)

PKI ensures a secure method for exchanging sensitive information over unsecured networks. In addition, PKI [39-41] provides authenticated, private and non-reputable communications.

PKI makes use of the technology known as public key cryptography. Public key cryptography uses a pair of keys to scramble and decipher messages, a public key and a private key. The public key is widely distributed whereas the private key is held secretly by an individual. Messages are protected from malicious people by scrambling them with the public key of the recipient. Only the recipient can decrypt the message by using his / her private key, thus retaining the privacy of the message. The public key is

distributed with a digital certificate that contains information that uniquely identifies an individual (for example name, email address, the date that the certificate was issued, and the name of the certificate authority which issued it). Also, by using digital certificates we can digitally sign messages to protect the integrity of the information itself and achieve non-repudiation (digitally signing a transaction is legally binding and no party can deny his /her participation).

PKI support is often integrated into common applications such as web browsers and email programs validating certificates and signed messages. The PKI can also be implemented by an organization for its own use to authenticate users that handle sensitive information. The digital certificate can be used by the user to either be authenticated to a mobile device or to the healthcare application in order to be able to access it and use the available services. Although the use of PKI counters many threats associated with public networks it also introduces management overhead and additional hardware and software costs that should be evaluated. An appropriate risk assessment should be performed in order to select the appropriate countermeasures to meet the organization's security requirements. Furthermore, there is a risk associated with the private key; the private key must be well-protected since if it is lost or compromised anyone could masquerade as the owner of the key.

#### 3.4.1.3 Smart card

Anything that is unique and that the user is required to possess can be used as an authenticating token [70]. A token is generally issued to one user. A token is registered to a user, and when it is presented for authentication, the token is verified as being legitimate. The identifying label of the token is used to verify its registration, if it has been lost or stolen, and if the user ID presented with it matches. If it is a match, the user is authenticated. Otherwise, the authentication request is rejected.

Tokens are generally made up of smart cards and Universal Serial Bus (USB) tokens. There is unique information stored on the token that identifies the possessor (i.e. a

private key). If a computer system accepts only the presentation of a token for authentication, then anyone who has that token can be authenticated. If the token is lost or stolen, entry can still be gained. However, passwords are employed with tokens to prevent this from happening. Thus, when a user wants to authenticate with a token, he/she inserts the token and then provides a password to unlock the credentials stored inside. The token and the password are used by the system to authenticate the user. This multi-factor authentication methodology still has the weaknesses of passwords because the token and associated password can be loaned or stolen. Still, simply knowing the password without the token is not sufficient for authentication. Both must be used together.

#### 3.4.1.4 Biometrics

Biometric [60] technology drives the future direction of strong authentication. The promise of biometrics to protect data and safeguard identity from being stolen is very compelling. Like any technology, it has needed time to mature and find its place in the computing infrastructure of enterprises. The time for biometrics has never been better. The industry and technology have matured, and the applications of biometrics are growing every day. From replacing the need for password authentication to strongly binding physical and digital identities, biometrics is being put to work.

A biometric is a physical or psychological trait that can be measured, recorded, and quantified. By doing this, we can use that trait to obtain a biometric enrollment. This way, we can say with a degree of certainty that someone is the same person in future biometric authentications based on their previous enrollment authentications.

Biometric user authentication can be accomplished using unique characteristics i.e. face, voice, fingerprint, and retinal. Mobile devices usually use fingerprint and voice biometric authentication to give access to the systems; these authentication methods use more compact devices that are suitable for the mobility aspect of mobile devices.

For example, fingerprint readers can be attached to the handheld devices through a serial or USB port and can be set to lock the whole device, to lock an individual application, or to connect to a remote database over a network or dial-up connection.

The strong advantage of biometrics is that they use something which is entirely unique and an adversary may not posse it in any way. However, depending on the authentication method used, biometrics have a different cost that must be evaluated against the need to implement such technology.

#### 3.4.1.5 Scenario

The following scenario describes how the authentication mechanisms are applied within the environment under evaluation.

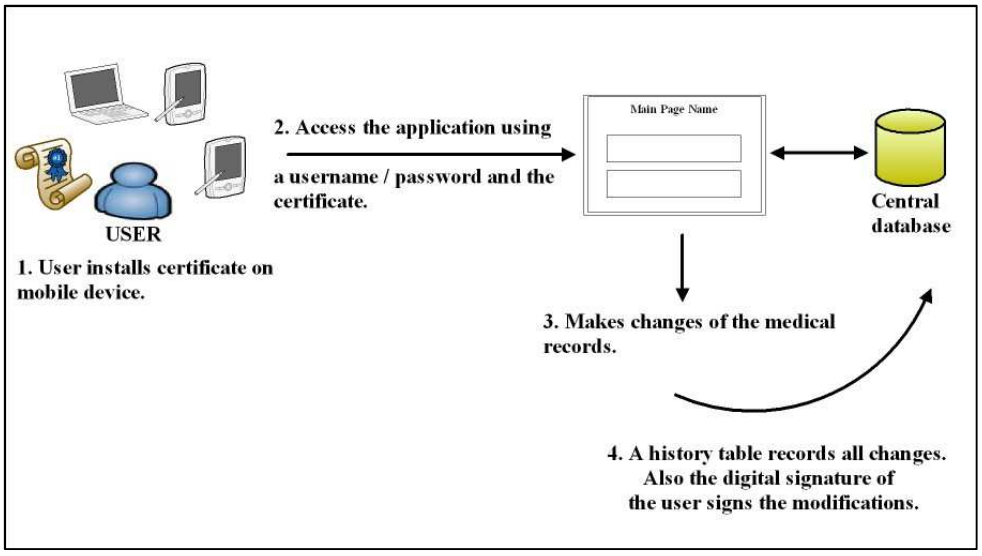


Figure 3.5: Authentication scenario

#### 3.4.2.1 Role separation

Access control [42,43] is essential for any system that handles sensitive information. As mentioned earlier, mobile healthcare services raise extra considerations since they

support the continuity of life. Therefore, healthcare information must be accessed on a need-to-know basis. Since a mobile healthcare application requires a fixed infrastructure to function that hosts a number of servers such as web and database servers, appropriate configurations must be made to provide access to data only to the designated personnel.

The most valuable asset of any healthcare application is the medical records that hold specific medical data about a patient i.e. health condition, medication treatment. This information is hosted and can be retrieved from the database server(s).

Role separation must be implemented to provide increased database security. Since the healthcare sector involves a number of medical professionals i.e. nurses, oncologists, physiotherapists, there is the need to distinguish the rights and permissions of each professional. Before deploying the application, it is essential to perform a detailed analysis in order to design access rights for each group of users. According to the organization, all appropriate user roles must be identified and their responsibilities must be documented in order to define their permissions. Based on the permissions defined, each group of users will have an appropriate view of the data stored on the database server.

#### 3.4.2.2 Scenario

The following scenario describes how the role separation is applied within the environment under evaluation.

Every user is mapped onto a user account. Users are mapped to User defined roles. Each group of users has a different view of the system according to the credentials assigned to the defined role.

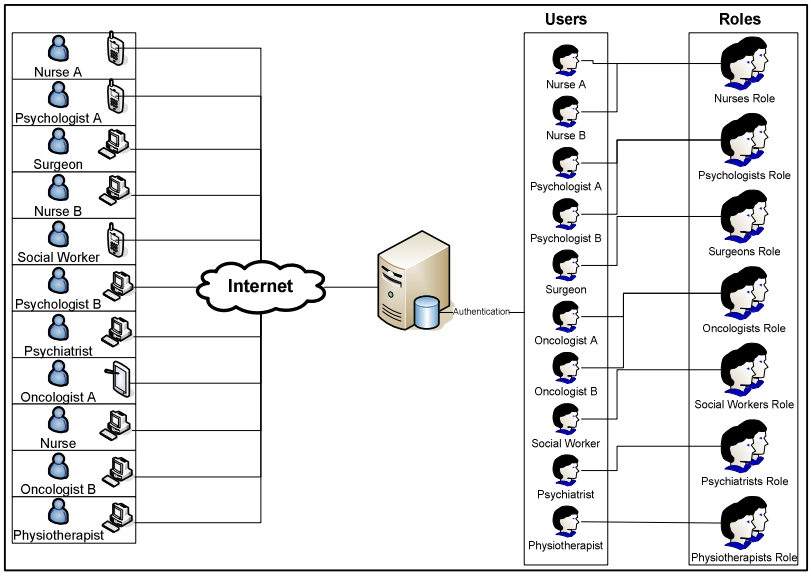


Figure 3.6: Role separation

### 3.4.3 Integrity & Confidentiality

#### 3.4.3.1 Encryption

There are many places where the data may be intercepted i.e. in thin-client, browser-based applications, email, data synchronization, and client / server communications. In order to retain the integrity and confidentiality of the data it is a necessity to implement end-to-end encryption between the mobile devices and the fixed infrastructure or implement encryption on the device to encrypt stored data that need protection. Encryption can be achieved by technologies such as PKI and Virtual Private Networks, which are discussed next.

#### 3.4.3.2 PKI

PKI [46] technology, which is discussed in 3.3.1.2 section, is used not only to authenticate a user but also to encrypt the information exchanged between two

communicating parties. The sender uses the digital certificate of the receiver to encrypt the information and then the receiver uses his / her private key to decrypt and read the information. Without the private key, the message is not possible to reconstruct to its original format.

#### 3.4.3.3 Virtual Private Networks (VPN)

As mentioned earlier, a fixed infrastructure is used to support the operations of the mobile healthcare application. There are situations where it is necessary for an administrator or a user to remotely access his / her desktop or other equipment. This must be done in a secure way, for example by implementing a virtual private network.

A VPN [47] allows a user to send data between two remote computers across a public network as he was using a point-to-point private link. Information sent over a VPN connection is kept private by using a tunnelling protocol and appropriate security procedures. Data is encrypted and encapsulated with a header containing routing information that is used to find its destination. In this way, even if the packets are intercepted, the attacker cannot read it or modify it without the changes be seen by the recipient. This functionality is what made companies use VPNs as sensitive information is still protected if someone manages to compromise the communication channel.

The following figure shows a typical VPN connection. Observe that the part of the connection in which the private data is encapsulated is known as the tunnel. The part of the connection in which the private data is encrypted is known as the virtual private network (VPN) connection.

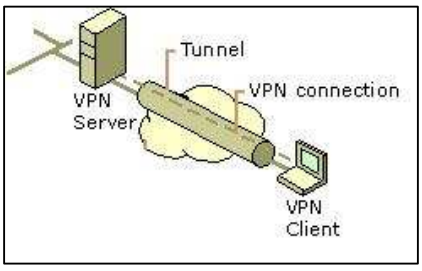


Figure 3.7: VPN

#### 3.4.3.4 Scenario

The following scenario describes how the PKI process will be applied within the environment under evaluation.

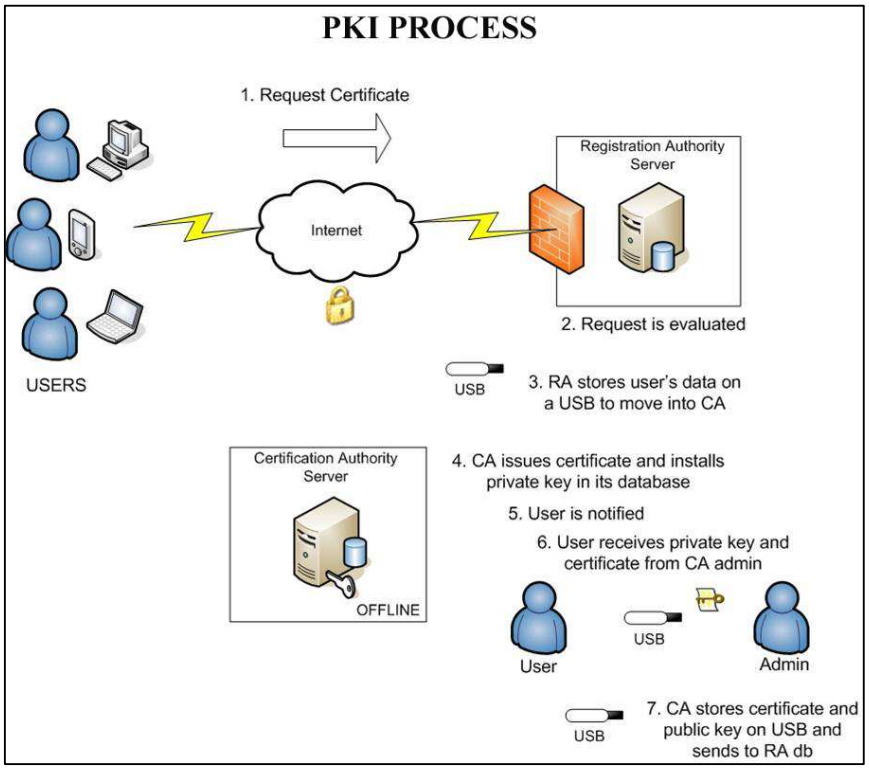


Figure 3.8: PKI process

### 3.4.4 Availability

Availability has always been an important characteristic of systems but becomes an even more critical and complex issue on networks. Healthcare sector operates on a 24 / 7 basis. Therefore, the flow of information must be continuous and not break off in any way.

This requirement is crucial, especially when maintaining a mobile healthcare application. In many cases, medical professionals like nurses may visit patients who are

located away from a fully equipped hospital and use their mobile device to connect with the hospital's database and retrieve information about the patient. This communication must be retained at all times so that nurses can respond immediately to emergencies.

#### 3.4.4.1 Fail Safe Plan

In sensitive areas like the healthcare sector, the implementation and operation of healthcare applications must be performed in a well-designed environment. The main idea is to be precautious and have a fail safe plan implemented so that if anything happens (due to physical threats like fires or a security violation) with the primary infrastructure, a secondary infrastructure will take over until the problem is solved; this means that equipment must be redundant so that operation will continuously be supported. This plan may introduce overhead in managing the two infrastructures but it is a cost that needs to be taken since the benefit to be gained is more important.

#### 3.4.4.2 Backups

In order to support a fail safe plan, it is necessary to maintain appropriate backups of the critical data hosted on systems. Data to be backuped may include medical records, security configurations and any other data that is considered to be critical for operation and must be accessible in a 24 / 7 basis. Data must be stored on removable media or other redundant equipment that are well protected (i.e. locked down) and be used immediately if a system crashes and goes down. Usually, backup copies are stored in a separate facility or in a fire-rated container that is not co-located with the operational software. Frequency of backing up is dependent upon how frequently the information is modified, as well as the criticality of the data. For instance, if the database is updated daily and if the organization would suffer operationally without the information in the database, then backups should be done on a daily basis.

#### 3.4.4.3 UPS

Since we are dealing with a network based application that requires an Internet connection to access services and resources, it is essential to guarantee the continuous provision of power supply. A UPS (Uninterruptible Power Supply) can be used to ensure the availability of systems and their operation.

#### 3.4.4.4 Scenario

The following scenario describes how availability could be achieved within the environment under evaluation. An appropriate secondary architecture is designed and will be implemented soon; if the primary architecture is unavailable, the redundant infrastructure will be used until the problem is solved. Currently, data is backuped on a daily basis.

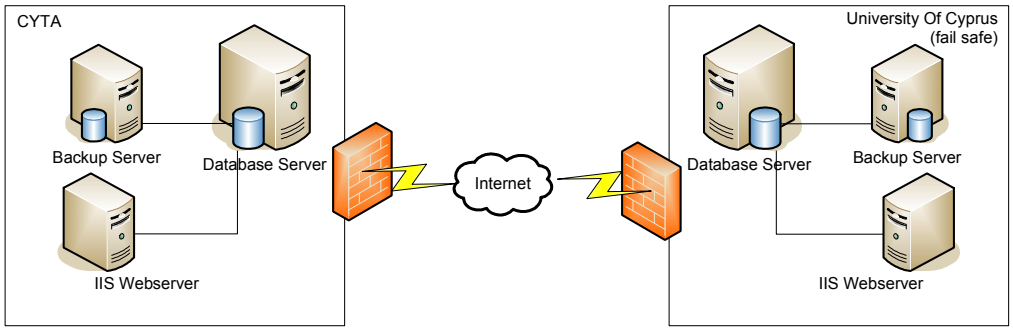


Figure 3.9: Fail Safe Plan

### 3.4.5 Non-repudiation

One of the biggest challenges in healthcare computing systems is to convince users that they will not be blamed for something they haven't done. For example, a doctor changes the medical treatment of a patient. The system must identify who made the change and also the details of the modification. The nurse is only responsible for

providing treatment according to the prescribed protocol; she is not responsible for its selection. Therefore, the system must implement appropriate mechanisms to ensure non-repudiating actions, where a user cannot later deny an action taken.

#### 3.4.5.1 History tables

As mentioned earlier, a mobile healthcare application is supported by a fixed infrastructure, where a variety of systems host sensitive data like the patients' medical records. Since it is important to record a number of events like who accessed certain information, who made a change and where, when a modification happened etc, it is essential to implement history tables on the database level.

The database server that hosts the data must be configured appropriately so that history tables are created. The history tables will contain all the recorded events so that a user action can be tracked down if necessary. For an enhanced level of security, the history tables must only be accessed by the administrator of the systems or other designated personnel; in addition to this, the tables must be encrypted so that noone who has access to the database server will be able to read and modify the tables.

#### 3.4.5.2 Digital signatures

A digital signature [46] has the same purpose as a handwritten signature. When a user digitally signs an electronic document (email, spreadsheet, text file etc.) he provides a mean to the recipient to authenticate him as the writer of the document. In addition, by receiving a digitally signed document a user can verify that it has not been altered in any way since the writer created it. The digital signature is created within the PKI framework.

The importance of using digital signatures is crucial to all B2B, B2C or C2C transactions as it guarantees non-reputable communication; this means that the

transacting parties cannot deny later on that they performed a specific action, for example a customer sending an order to a company.

Digital signatures are created and verified by public key cryptography. A user to send a digitally signed message to Bob must follow the procedure:

1. First the sender uses his signing software on the message to compute a message digest. This process is called hashing. Have in mind that the process is irreversible meaning that it is impossible to change the message digest back into the original data from which it was created.
2. Then the user uses the signing software to encrypt the message digest with his private key. Doing so, he creates his digital signature.
3. The signing software appends the digital signature to the document. He then sends the message to his dear friend Bob.
4. Now that Bob has received the message will try to verify that it is sent by the indented sender and that the message has not been altered by a third party. So, Bob uses his software to decrypt the digital signature by using the user's public key, and gets the message digest.
    a. If the decryption is successful Bob knows that the user signed the document. After all he is the only one who has the corresponding private key to the public key Bob used.
5. Then, Bob uses his software to compute the message digest (also known as hash value) of the received message.
6. The software checks that the computed message digest is the same with the message digest created when the digital signature was decrypted.
    a. If the verification is successful Bob knows that noone has altered the signed message.

By using digital signatures in a healthcare application, we achieve non-repudiating actions. For example, a doctor changing the medical treatment of a patient cannot later deny his action. However, it is important to educate the users about issues like the importance of protecting the private key; if someone else compromises the key then he would be able to sign documents on behalf of the user owning the key.

Furthermore, it is essential to make a background research and find out if the legislation supports the operation of digital signatures and whether such evidence is accepted by a court of law.

#### 3.4.5.3 Confidentiality documents

Although users must be convinced for the transparency of the communications, they also have responsibilities against patients and against the organization offering the healthcare services.

Medical personnel accessing medical information have a responsibility to maintain the privacy of the data. After all, a patient's reputation may be damaged if his medical condition is publicized, for example he could loose his job.

In addition to the medical personnel, the development personnel of the healthcare application may have access to confidential documents [48]. Therefore, it is critical to create confidentiality and code of ethics documents that must be signed by both medical and development personnel (Appendix B). By signing these documents, all personnel recognize the importance of keeping information confidential and also the responsibilities they have towards the organization. Note that the documents must adhere to local and national data protection laws.

To retain the non-repudiating objective, it is important to bind the patients as well. The patients must sign an appropriate form, acknowledging and permitting the storage and processing of their personal and medical information for providing an enhanced quality of care. In this way, the healthcare team is legally covered in a case of a lawsuit.

### 3.4.6 Security awareness and training

Security awareness is often an overlooked element of security management because most of a security practitioner's time is spent on controls, intrusion detection, risk assessment, and proactively or reactively administering security.

It should not be that way, however. People are often the weakest link in a security chain because they are not trained or generally aware of what security is all about. Employees must understand how their actions, even seemingly insignificant actions, can greatly impact the overall security position of an organization.

Employees must be aware of the need to secure information and to protect the information assets of an enterprise. Operators need training in the skills that are required to fulfill their job functions securely, and security practitioners need training to implement and maintain the necessary security controls.

All employees need education in the basic concepts of security and its benefits to an organization. The benefits of the three pillars of security awareness training -awareness, training, and education - will manifest themselves through an improvement in the behavior and attitudes of personnel and through a significant improvement in an enterprise's security.

The purpose of computer security awareness, training, and education is to enhance security by:

- Improving awareness of the need to protect system resources
- Developing skills and knowledge so computer users can perform their jobs more securely
- Building in-depth knowledge, as needed, to design, implement, or operate security programs for organizations and systems

An effective computer security awareness and training program requires proper planning, implementation, maintenance, and periodic evaluation. In general, a computer security awareness and training program should encompass the following seven steps:

1. Identify program scope, goals, and objectives.
2. Identify training staff.
3. Identify target audiences.
4. Motivate management and employees.
5. Administer the program.
6. Maintain the program.
7. Evaluate the program.

Making computer system users aware of their security responsibilities and teaching them correct practices helps users change their behavior. It also supports individual accountability because without the knowledge of the necessary security measures and how to use them, users cannot be truly accountable for their actions.

### 3.4.7 Physical security

Physical security [49] controls are implemented to protect the facility housing system resources, the system resources themselves, and the facilities used to support their operation.

Physical security controls include the following three broad areas:

1. The physical facility is usually the building, other structure, or vehicle housing the system and network components. Systems can be characterized, based upon their operating location, as static, mobile, or portable. Static systems are installed in structures at fixed locations. Mobile systems are installed in vehicles that perform the function of a structure, but not at a fixed location. Portable systems are not installed in fixed operating locations. They may be operated in

wide variety of locations, including buildings or vehicles, or in the open. The physical characteristics of these structures and vehicles determine the level of such physical threats as fire, roof leaks, or unauthorized access.

2. The facility's general geographic operating location determines the characteristics of *natural threats*, which include earthquakes and flooding; *man-made threats* such as burglary, civil disorders, or interception of transmissions and emanations; and *damaging nearby activities*, including toxic chemical spills, explosions, fires, and electromagnetic interference from emitters, such as radars.
3. Supporting facilities are those services (both technical and human) that underpin the operation of the system. The system's operation usually depends on supporting facilities such as electric power, heating and air conditioning, and telecommunications. The failure or substandard performance of these facilities may interrupt operation of the system and may cause physical damage to system hardware or stored data.

In this study, the investigation concerns physical access controls that restrict the entry and exit of personnel (and often equipment and media) from an area, such as an office building, suite, data center, or room containing a LAN server.

The controls over physical access to the elements of a system can include controlled areas, barriers that isolate each area, entry points in the barriers, and screening measures at each of the entry points. In addition, staff members who work in a restricted area serve an important role in providing physical security, as they can be trained to challenge people they do not recognize.

Physical access controls should address not only the area containing system hardware, but also locations of wiring used to connect elements of the system, the electric power service, the air conditioning and heating plant, telephone and data lines, backup media and source documents, and any other elements required system's operation. This means that all the areas in the building(s) that contain system elements must be identified.

It is also important to review the effectiveness of physical access controls in each area, both during normal business hours, and at other times particularly when an area may be

unoccupied. Effectiveness depends on both the characteristics of the control devices used (e.g., keycard-controlled doors) and the implementation and operation. Statements to the effect that "only authorized persons may enter this area" are not particularly effective. Organizations should determine whether intruders can easily defeat the controls, the extent to which strangers are challenged, and the effectiveness of other control procedures. Factors like these modify the effectiveness of physical controls.

A number of physical security devices exist and can be used to prevent unauthorized access, intentional damage or destruction, or theft of computer equipment and components such as alarms, locks, cabinets, cable kits, lock down plates and special security screws.

In the case of portable and mobile systems, they share an increased risk of theft and physical damage. In addition, portable systems can be "misplaced" or left unattended by careless users. Secure storage of portable and mobile systems is often required when they are not in use. If a mobile or portable system uses particularly valuable or important data, it may be appropriate to either store its data on a medium that can be removed from the system when it is unattended or to encrypt the data.

### 3.4.8 Auditing

Auditing [71] is used to check systems to see whether a particular system is meeting stated security requirements, including system and organization policies, and whether security controls are appropriate. Informal audits can be performed by those operating the system under review or, if impartiality is important, by outside auditors.

Thus, audits can be self-administered or independent (either internal or external). Both types can provide excellent information about technical, procedural, managerial, or other aspects of security. The essential difference between a self-audit and an independent audit is objectivity. Reviews done by system management staff, often called self-audits/assessments, have an inherent conflict of interest. The system

management staff may have little incentive to say that the computer system was poorly designed or is sloppily operated. On the other hand, they may be motivated by a strong desire to improve the security of the system. In addition, they are knowledgeable about the system and may be able to find hidden problems.

The independent auditor, by contrast, should have no professional stake in the system. Independent audit may be performed by a professional audit staff in accordance with generally accepted auditing standards.

There are two types of automated audit tools: (1) active tools, which find vulnerabilities by trying to exploit them, and (2) passive tests, which only examine the system and infer the existence of problems from the state of the system.

Automated tools can be used to help find a variety of threats and vulnerabilities, such as improper access controls or access control configurations, weak passwords, lack of integrity of the system software, or not using all relevant software updates and patches. These tools are often very successful at finding vulnerabilities and are sometimes used by hackers to break into systems. Not taking advantage of these tools puts system administrators at a disadvantage. Many of the tools are simple to use; however, some programs (such as access-control auditing tools for large mainframe systems) require specialized skill to use and interpret.

### 3.4.9 Security Policies

In order to ensure that computer systems are used in an effective and productive way, it is important that the owners, operators and users of these systems have a clear understanding of acceptable standards of use. The primary step in securing an electronic system is developing and implementing a variety of security policies [50,72].

Security policies are the foundation and the bottom line of information security in an organization. A well-written and implemented policy contains sufficient information on

what must be done to protect information and people in the organization (Appendix A). It is important to establish who the authorized users might be, how they will access the system and data, how unauthorized users will be denied access, and how data will be protected within the organization as well as outside the organization. In general, thoroughly planned security policies set directions and procedures as well as define penalties and countermeasures if the policy is transgressed.

In order for a security policy to be viable for the long term, it requires a lot of flexibility based upon an architectural security concept. A security policy should be (largely) independent from specific hardware and software situations (as specific systems tend to be replaced or moved overnight). The mechanisms for updating the policy should be clearly spelled out. This includes the process, the people involved, and the people who must sign-off on the changes.

Once the security policy has been established it should be clearly communicated to users, staff, and management. Having all personnel sign a statement indicating that they have read, understood, and agreed to abide by the policy is an important part of the process. Finally, the policy should be reviewed on a regular basis to see if it is successfully supporting your security needs.

Following, a variety of policies that could be implemented according to each situation are listed:

- Password policy
- Anti-virus policy
- Email policy
- Encryption policy
- Remote access policy
- Audit policy
- Internet access policy
- Intrusion detection policy
- Security incident handling policy
- Portable and mobile systems usage

### 3.4.10 Security tools

A variety of security tools exist to support and maintain security of systems.

#### 3.4.10.1 Anti-virus

If there's one word that can strike fear in the heart of any computer user, especially one who accesses the internet, or exchanges diskettes, that word is, "virus." Viruses can generate so much fear in the cyber world that news of a new virus often spreads faster than the virus itself. On line viruses are a fact of internet life. Anti-virus programs are the most effective means of fighting viruses. Anti-virus software is cheap, easy insurance against outside attackers. Basic anti-virus software works by scanning stored files on a computer for the telltale signatures of viruses. The principle of operation of anti-virus scanners is based on checks of files, sectors and system memory, and search for known and new (unknown to scanner) viruses.

There are two primary components to anti-virus software: the virus-scanning engine (which performs the virus check) and the data files (which tell the scanning engine what to look for). Data files are updated more frequently than scanning engines, but both components do need to be updated. Two companies dominate the anti-virus market: Symantec, makers of Norton AntiVirus and Network Associates, publishers of McAffee Anti-Virus.

#### 3.4.10.2 Firewall

The most common building block of an effective security architecture is the firewall approach. Firewalls constitute the first line of defense for the enterprise’s interface with the external (i.e. internet) environment in protecting private information. The Internet is a volatile and unsafe environment, therefore a firewall must be positioned to control all

incoming and outgoing traffic and enhance the safeguard of the enterprise's assets from any threat that may come from the net.

Several kinds of firewalls are available and each has its merits and drawbacks. The key to successfully implementing a firewall is finding the kind of firewall that best suits a particular network's needs. There are two basic types of firewall, or two ways a firewall can function: Packet filter or proxy firewalls. Within each type, though, are different implementations.

A packet filter rests between the internal network and the rest of the world. Clients and servers connect directly, but the packets pass through the packet filter to travel between the internal network and the outside world. When packets pass through, the packet filter compares the packets to a set of filter rules (criteria such as service type, port number, interface number, source address, and destination address). If the configuration is set up to permit a packet, it continues its travels through the network, forwarded on to its next hop. If the configuration does not permit the packet, it is discarded.

On networks with packet filters, a connection is formed directly between the client and the server. Proxies break up the connection between the client and the server. The proxy server type of firewall attempts to hide the configuration of the network behind the firewall by acting on behalf of that network, or as a "proxy." All requests for access are translated at the firewall so that all packets are sent to and from the firewall, rather than from the hosts behind the firewall. No direct communication takes place between the client and the server. If an attacker tries to play tricks by working with fragmented packets or fields in the IP packet, the internal server never sees it.

#### 3.4.10.3 Intrusion detection system

As exposure and risks increase, organizations seek new ways to improve their network security. Most commonly we hear of firewalls, authentication tools, and antivirus

applications, but the generally accepted best practice of defense in depth requires more, hence the recent attention being paid to Intrusion Detection Systems (IDSs).

With the number of intrusion and hacking incidents around the world on the rise, the importance of having dependable intrusion detection systems in place is greater than ever. Offering both a developmental and technical perspective on this crucial element of network security, Intrusion Detection covers: practical considerations for selecting and implementing intrusion detection systems; methods of handling the results of analysis, and the options for responses to detected problems, data sources commonly used in intrusion detection and how they influence the capabilities of all intrusion detection systems; legal issues surrounding detection and monitoring that affect the design, development, and operation of intrusion detection systems. More than just an overview of the technology, Intrusion Detection presents real analysis schemes and responses, as well as a detailed discussion of the vulnerabilities inherent in many systems, and approaches to testing systems for these problems.

Intrusion Detection Systems function alerting to intrusions and attacks aimed at computers or networks. They are your eyes and ears, essential in knowing whether you are under attack. Traditionally, there have been two main classes of intrusion detection systems: host-based and network-based systems.

A host-based intrusion detection system monitors the detailed activity of a particular computer host in real-time. Host-based systems were the development of network-based intrusion detection systems. While some network-based system focus on a single host, most typically monitor a network of computers and other devices (i.e. routers, gateways) that are subject to attacks. The IDS system attempts to detect known attack "signatures" or attack patterns within the activity of computer's operation and notify accordingly the administrator.

### 3.5 Security based on Information Classification

There are several good reasons to classify information. Not all data has the same value to an organization. Some data is more valuable to the people who are making strategic decisions because it aids them in making long-term or short-term business direction decisions. Some data, such as trade secrets, formulas, and new product information, is so valuable that its loss could create a significant problem for the enterprise in the marketplace by creating public embarrassment or by causing a lack of credibility. Furthermore, in a healthcare environment the well being (in certain cases it can even be life threatening) of patients depends on it. For these reasons, it is obvious that information classification has a higher, enterprise-level benefit. Information can have an impact on a business globally, not just on the business unit or line operations levels. Its primary purpose is to enhance confidentiality, integrity, and availability, and to minimize the risks to the information. In addition, by focusing the protection mechanism and controls on the information areas that need it the most, a more efficient cost-to-benefit ratio is achieved.

A number of guides [51-54] exists today providing information on how to classify confidential information for a variety of sectors like the government and the healthcare sector. Furthermore, a variety of formal security models have been developed to model access control requirements to specific resources through a defined security policy. The Bell-La Padula [55] framework models access control requirements focusing on the confidentiality of classified information; the Biba framework [56] models a set of access control rules designed to ensure that data are not contaminated; the Brewer-Nash [57] framework models access control requirements that can change dynamically; the Graham and Denning [58] framework models a set of basic rights on how specific subjects can execute security functions on an object.

Through out our research, no security framework has been detected modelling the implementation of security technologies according to information's classification sensitivity, particularly in the healthcare environment. However, healthcare security frameworks exist, although that they do not take into consideration information

classification. Markovic et al. [32] overview modern security systems which are used in medical electronic business systems and mobile healthcare systems. Bourka et al. [41] describe and assess the integration of Public Key Infrastructure security mechanisms (such as strong authentication and encryption) in an electronic referral and prescription application. Spinellis et al. [59] proposed a secure framework for web-based telemedical applications defining among others the relationship between security services and security concepts and technologies. Misra et al. [5] address the security challenges raised by mobile communication and discuss the wired equivalent security showing how this concept can be applied to achieve end-to-end security in a mobile healthcare environment.

In this section, we propose a security-level information classification scheme [67] associated with the appropriate security technologies and the objective these technologies serve, that can be adopted in a healthcare environment. The proposed scheme aims to balance the trade-off between security complexity and performance. In this way, implementing a complex and flat security architecture that will degrade the performance of the provided services can be prevented. Security technologies must be used in a smart and efficient way in order to balance security complexity and performance.

### 3.5.1 Information classification benefits

Information classification has the longest history in the government sector. Its value has been established, and it is a required component when securing trusted systems. In this sector, information classification is primarily used to prevent the unauthorized disclosure and the resultant failure of confidentiality.

Information classification can be used in any sector to comply with privacy laws, or to enable regulatory compliance. A company may wish to employ classification to maintain a competitive edge in a tough marketplace. There may also be sound legal

reasons for a company to employ information classification, such as to minimize liability or to protect valuable business information.

In addition to the reasons mentioned previously, employing information classification has several clear benefits to an organization. Some of these benefits are as follows:

- Demonstrates an organization's commitment to security protections
- Helps identify which information is the most sensitive or vital to an organization
- Supports the tenets of confidentiality, integrity, and availability as it pertains to data
- Helps identify which protections apply to which information
- May be required for regulatory, compliance, or legal reasons

### 3.5.2 Information classification concepts

According to the Council of Europe Recommendation R(97)5 on the Protection of Medical Data "*Appropriate technical and organizational measures shall be taken to protect personal data - processed in accordance with this recommendation - against accidental or illegal destruction, accidental loss, as well as against unauthorized access, alteration, communication or any other form of processing. Such measures shall ensure an appropriate level of security taking account, on the one hand, of the technical state of the art and, on the other hand, of the sensitive nature of medical data and the evaluation of potential risks*."

It is obvious that the medical data is placed on the center of all efforts towards security. The information produced or processed by an organization must be classified according to the organization's sensitivity to its loss or disclosure. This approach enables the security controls to be properly implemented according to its classification scheme.

As stated earlier, a number of guides [51-54] provide guidance on how to classify [61-63] confidential information.

The proposed healthcare security framework defines a four level classification based on the aforementioned guides:

1. Public level. Information is categorized in the public level if it is intended to be used by any interested party. This level includes: educational material, press releases, annual reports, and statistics. The public release of this information does not violate security requirements; therefore, security mechanisms are not needed for this level.
2. Internal Use Only level. Although this information is intended to be used internally, compromization will not impact the organization. Internal Use Only information involves demographics, internal reports, appointments and the virtual team assigned to each patient. Security is required but can be kept at minimum levels.
3. Confidential level. This category involves patients' medical records that are accessed by appropriate personnel on a need-to-know basis. Medical records include, among others, information on medical history, symptoms, diagnosis, treatment and medication. Security at this category must be highly defined.
4. Highly confidential level. This level involves medical records of special content such as information related to physical abuse, HIV status, and abortions. Furthermore, it includes medical records of recognized people (such as the president of a country) that their work position is considered critical.

Information was classified according to ISO/ IEC17799 [64] recommendations; information should be labelled according to how:

- valuable
- sensitive
- critical it is

and how much protection it needs.

### 3.5.3 Security-level Information Classification Scheme

As discussed earlier, labeling information into sensitivity classes can help us provide the appropriate protection by applying the necessary security measures for each situation. A number of formal security models exists that define the access control rights a subject may have on a specified category of information, according to the access control profile that is assigned to it. However, security frameworks do not exist associating information classification with the required security technologies that are needed to be implemented based on information's sensitivity. By developing such a framework, our aim is to provide guidance on the minimum measures/ technologies that are needed to be implemented without saturating the performance of the entire system/ application.

Table 2 indicates the relationship between the classification of information, the security objectives and technologies discussed in the previous sections. All these, formulate a security-level classification scheme of information associated with the appropriate security technologies and the objective these technologies serve, that can be adopted in a healthcare environment. The scheme defines the *minimum guidelines* that should be followed to safeguard the information classified under each level.

For Public-level information, security is seamless since this type of information can be used by anyone who has an interest on it. Minimum security measures that can be applied are: a monthly backup of the information that for example resides on the web server; frequency of backing up is dependent upon how frequently the information is modified, as well as the criticality of the data. Physical security measures such as access control to facilities are recommended to safeguard the systems/ machines that are hosting this kind of information. Although the scheme does not address integrity issues on this level, the organization, according to its needs, may require that information classified under public level must be accurate. If this is the case, then appropriate security must be applied i.e. encryption.

For Internal-Use-Only-level information, security is required on a basic level. Access to this kind of information should be controlled through appropriate user profiles that are assigned to users that provide their username and password to get verified by the

system. Simple history logs should be kept in order to have a view of the people that access specific information; backups can be taken at least twice a week since information like appointments and internal reports are defined within the week. The backup scheme is always depended on the organization's needs and requirements and someone cannot say with accuracy how frequently the backup should be. If the organization is operated in a way that, for example, daily reports are created backing up the system may be needed on a daily basis. Also physical security is necessary to protect unauthorized access to servers and other equipment.

For Confidential-level information, security must cover at least the principle security technologies/ measures listed under each security objective. Information that is classified under this category is a valuable asset for the organization and it needs to be protected. Users should use basic authentication to access the system based on the access-right profile assigned to them and any communication established between the users and the infrastructure using public networks should be encrypted. Appropriate changes made on medical records should be digitally signed to achieve accountability on users' activities. History logs should be maintained to control access to the systems, failures etc. This kind of information should be audited frequently, as well as the entire system, in order to ensure that the implemented security measures are adequate. Medical professionals should sign appropriate confidentiality documents recognizing their responsibility in protecting the privacy of medical records. Backups should be applied at least twice a day. Frequency of back up will be dictated by ability of person using the system to recall their entries. For example, we assume that a health professional changing a medication entry for a patient can recall the change he made, if he is asked to within the next few hours. However, this is a complex subject and a matter of further research. Physical security is required as previously and finally a fail safe plan must be in place so if the primary infrastructure is unavailable, a secondary infrastructure will be used in order to provide access to medical records that may be needed in urgent situations.

For Highly-Confidential-level information, a complete and sound security implementation must be provided; in this case, the security framework must implement all the security techniques/ measures that are listed under each security objective of the

table. This category includes all the measures discussed in the previous category and in addition it implements smart card and/ or biometric technologies to be used by 2 key-people personnel to access top-secret medical information.

| OBJECTIVES | TECHNOLOGIES | CLASSIFICATION | | | |
|---|---|---|---|---|---|
| | | **Public Level** | **Internal Use Only** | **Confidential Level** | **Highly Confidential** |
| **I&C** | Encryption (PKI,VPN) | NO | NO | YES | YES |
| **Availability** | Fail Safe Plan | NO | NO | YES | YES |
| | Backups | YES (2/ month) | YES (2/week) | YES (2/day) | YES (2/day) |
| **A&A** | Password | NO | YES | YES | YES |
| | PKI | NO | NO | YES | YES |
| | Smart Card | NO | NO | NO | YES |
| | Biometrics | NO | NO | NO | YES |
| **Accountability** | History | NO | YES | YES | YES |
| | Digital Signatures | NO | NO | YES | YES |
| | Confidentiality docs | NO | NO | YES | YES |
| | Auditing | NO | NO | YES | YES |
| **Logical Access** | Role Separation | NO | YES | YES | YES |
| **Physical Access** | Physical Security | YES | YES | YES | YES |
| I&C = Integrity & Confidentiality, A&A = Authentication & Authorization | | | | | |

Table 2: Security-level information classification scheme

# Chapter 4

## Evaluation



### 4.1 Introduction

Users need confidence in the security of the system they are using. The system's security capabilities and procedures must represent the security needs and requirements of users that rely on the system to perform their job well. Although users could rely upon the word of the vendors of the systems, most users prefer to rely on the results of some form of assessment conducted by an independent body. For a system, an evaluation of its security capabilities can be viewed as a part of a more formal procedure for accepting an IT system for use within a particular environment. Accreditation is the term often used to describe this procedure. It requires a number of factors to be considered before a system can be viewed as fit for its intended purpose: it requires assurance in the security provided by the system, a confirmation of management responsibilities for security, compliance with relevant technical and legal/regulatory requirements, and confidence in the adequacy of other non-technical security measures provided in the system environment. Such an evaluation of a system requires objective and well-defined security evaluation criteria that are going to be used to measure the appropriateness of the system.

The evaluation of the proposed security framework is still in progress as DITIS security is still in the development phase. However, we could assess the completeness of the framework against well-known practices.

The proposed framework will be evaluated against the ISO/ IEC 17799 [64] standard that defines the code of practice for information security management. The result of the evaluation is expected to show if the proposed security framework implements adequate techniques and procedures providing the needed protection in the healthcare environment, and particularly for the system in question.

**4.2 ISO/ IEC 17799**

ISO/IEC 17799 is an information security standard published in 2005 by the International Organization for Standardization and the International Electrotechnical Commission. It is entitled *Information technology - Security techniques - Code of practice for information security management*. The current standard is a revision of the version published in 2000, which was a word-for-word copy of the British Standard BS 7799-1:1999.

ISO/IEC 17799 provides best practice recommendations on information security management for use by those who are responsible for initiating, implementing or maintaining information security management systems. Information security is defined within the standard as *the preservation of confidentiality (ensuring that information is accessible only to those authorized to have access), integrity (safeguarding the accuracy and completeness of information and processing methods) and availability (ensuring that authorized users have access to information and associated assets when required)*.

The standard contains the following sections:

- Security policy
- Organization of information security
- Asset classification and control
- Personnel security
- Physical and environmental security
- Communications and operations management
- Access control
- Systems development and maintenance
- Business continuity management
- Compliance

Within each section, information security objectives are specified and a range of

controls are outlined that are generally regarded as best practice means of achieving those objectives. For each of the controls, implementation guidance is provided. Specific controls are not mandated since (a) each organization is expected to undertake a structured information security risk assessment process to determine its requirements before selecting controls that are appropriate to its particular circumstances and (b) it is practically impossible to list all conceivable controls in a general purpose standard.

### 4.3 Evaluation analysis

ISO/IEC 17799 is a code of practice. As such, it addresses topics in term of policies and offers guidelines for information security management. It is meant to provide a high level, general description of the areas currently considered important when initiating, implementing or maintaining information security in an organization. It is noted, however, that the standard is a starting point for developing organization guidance and additional security controls not contained may be required.

Since it is not feasible to conduct a complete system-technical evaluation as DITIS has not reached its final operational state and security is still an on-going activity, ISO/ IEC 17799 has been selected to be used for evaluating the proposed security framework. The standard deals with the examination of non-technical issues related to personnel, procedural, physical security and security management in general. Therefore, it could be useful as a high-level evaluation of the proposed security framework since it is not practical yet to perform a technical evaluation of DITIS security features.

The standard addresses specific guidelines for each one of the areas listed in section 4.2. Each security area defined in the standard will be used against the techniques and measures presented in the proposed framework, evaluating if the framework adequately covers the objectives listed under each of these area. The evaluation will be applied on a high level and will not assess technical details. An appropriate analysis follows comparing the objectives and guidelines within each section of the standard with the security techniques and procedures proposed in our framework. At the end, the evaluation will identify the areas of the proposed framework that need to address additional security measures in order to meet the objectives of the ISO/ IEC 17799 standard.

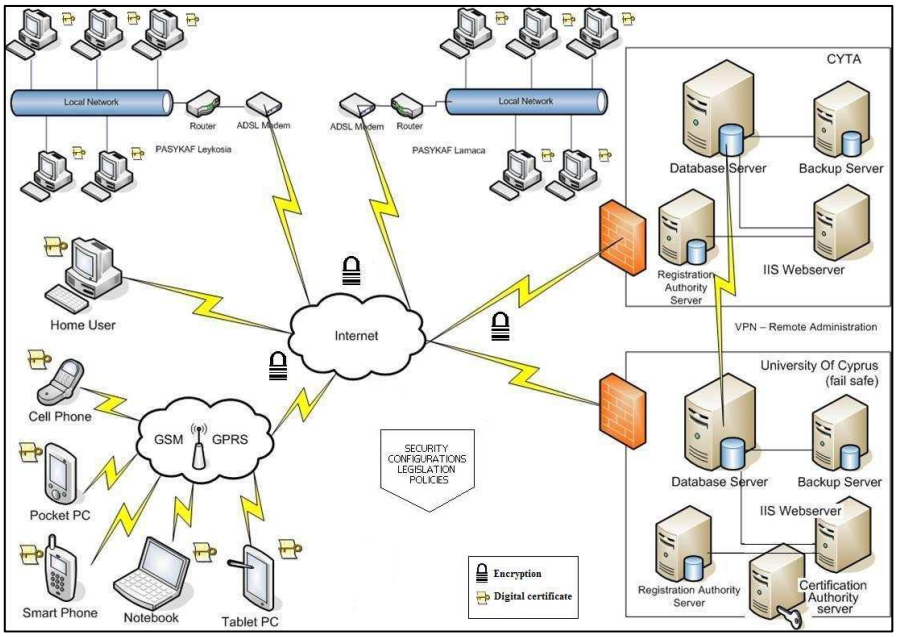


Figure 4.1: Security aspects of DITIS

### 4.3.1 Security policy

The objective of this area is to provide management direction and support for information security in the organization. Throughout the standard, it appears that there is the need to design a variety of security policies, covering many technical and non-technical aspects of a system.

The proposed security framework provides a template for designing a set of security policies; password, antivirus, email, encryption, remote access, audit and internet access policy is covered. The actual security policies are expected to be finalized when DITIS reaches an operational level. However, some samples of template documents which will form part of the Security Policy document for DITIS are provided in Appendix A.

### 4.3.2 Organization of information security

Organization of information security involves the management of the information security within the organization. A management framework should be established to initiate and control the implementation of information security within the organization. Suitable management should be established to approve the information security policy, assign security roles and coordinate the implementation of security across the organization. Furthermore, this section defines that access to the organization's information assets by third parties such as IT service providers, maintenance and support staff, consultants and contractors should be controlled. Information security requirements should be included in contracts with such third parties.

The proposed security framework does not explicitly define a security management framework; rather it focuses on the security techniques and procedures that could be applied. However, since information security is a business responsibility shared by all members of the management team, a clear direction and visible management support for security initiatives should therefore be considered. The security management should be responsible for the following:

- Reviewing and approving information security policy and overall responsibilities
- Monitoring significant changes in the exposure of information assets to major threats
- Reviewing and monitoring information security incidents
- Approving major initiatives to enhance information security

Regarding third-party access to the organization's information assets, appropriate legal documents are created based on European and local data protection laws that third-party users must sign, recognizing their responsibility of protecting the organization's assets. These documents can be found in Appendix B.

### 4.3.3 Asset classification and control

The objective of this section is to provide guidance on protecting the organizational assets. It firstly defines that all major information assets should be accounted for and have a nominated owner. *Accountability for assets* helps to ensure that appropriate protection is maintained. Furthermore, *information classification* is needed to ensure that information assets receive an appropriate level of protection. Information should be classified to indicate the need, priorities and degree of protection. Information has varying degrees of sensitivity and criticality. An information classification system should be used to define an appropriate set of protection level, and communicate the need for special handling measures.

Our framework makes use of the OCTAVE risk evaluation methodology to identify the risks associated with DITIS environment and operation. Throughout the risk evaluation process, the assets of the organization were identified as well as how valuable they are for the organization. Based on this information the organization can then provide levels of protection commensurate with the value and importance of the assets. The proposed framework also defines an appropriate information classification scheme that determines how the information is to be handled and protected; labeling of information is defined in terms of information's value and sensitivity to the organization.

### 4.3.4 Personnel security

Personnel security aims in reducing the risks of human error, theft, fraud or misuse of the organization's assets. All employees and third-party users of information processing facilities should sign a confidentiality (non-disclosure) agreement. Furthermore, user training is required to ensure that users are aware of information security threats and concerns, and are equipped to support organizational security policy in the course of their normal work. In addition, users should be trained in security procedures and the correct use of information processing facilities to minimize possible security risks.

Finally, this section defines the need of having appropriate procedures to respond to security incidents and malfunctions.

The proposed security framework addresses personnel security with the design of 1) appropriate confidentiality agreements and code of ethics documents that are signed by all individuals working for the organization (samples are provided in Appendix B), 2) an education and training framework that provides guidelines for creating awareness activities within the organization and 3) incident response policy that defines the procedures for reporting an incident as quickly as possible to the designated point of contact. An appropriate template policy which will be used in DITIS Security policy is included in Appendix A.

### 4.3.5 Physical and environmental security

The objective of this area covers the need to prevent unauthorized access, damage and interference to organization's premises and information. Sensitive information processing facilities should be housed in secure areas, protected by a defined security perimeter, with appropriate security barriers and entry controls. The protection provided should be commensurate with the identified risks.

The proposed framework covers physical security on a high level, providing the principle concepts that should be addressed in the organization's environment. More detailed guidelines should be addressed in the actual environment, after taking into consideration the organization's facilities.

### 4.3.6 Communications and operations management

This section covers security aspects of IT systems and network operations activities. It identifies the need of having operations procedures and responsibilities to ensure the correct and secure operation of the system. The procedures cover incident management

procedures, monitoring activities, system acceptance criteria, controls against malicious software, backup routines, network security, and email security.

The proposed framework addresses the aforementioned issues. Incident management procedures are provided through an appropriate security policy document, history and logs are implemented to provide monitoring over users' activities, guidelines are defined on how to establish tests of the system prior to its acceptance, usage of antivirus and auditing tools will protect from malicious software, backup is defined in the information classification scheme, encryption will protect the information exchanged over the network as well as provide for email security.

### 4.3.7 Access control

Access to information should be controlled to safeguard the information from malicious alterations or disclosure.

The proposed security framework implements a number of access control mechanisms. Appropriate user profiles are defined on the database level, providing access to certain aspects of the information; a user is accessing only the information he has a need-to-know. Each profile is associated with a certain job function i.e. nurse, social worker etc, that gives access to the necessary information that is needed for the user to do his/ her job. Furthermore, simple access control (username/ password) is implemented to provide access to non-critical data while advanced access control (digital certificates/ smart card/ biometrics) is defined based on the sensitivity level of the information. Furthermore, event logging is defined to detect deviation from access control policy and record events to provide evidence in case of security incidents. The framework should be upgraded to provide specific guidelines to ensure security when using mobile computing. A formal policy should be adopted that takes into account the risks of working with mobile equipment, in particular in unprotected environments. For example such a policy could include the requirements for physical protection, access controls, cryptographic techniques, back-ups and virus protection. Currently, DITIS

implements simple access control based on role separation and audit logs. Advanced access control using digital certificates is still under testing.

### 4.3.8 Systems development and maintenance

The objective of this area is to ensure that security is build into information systems; this includes infrastructure and applications. The design and implementation of the business process supporting the application or service can be crucial for security. Security requirements should be identified and agreed prior to the development of the information system. Appropriate controls and audit trails or activity logs should be designed into application systems. These should include the validation of input data, internal processing and output data. Cryptographic systems and techniques should be used for the protection of information that is considered at risk and for which other controls do not provide adequate protection.

As mentioned, the security framework makes use of the OCTAVE risk evaluation methodology to identify the security requirements that need to be addressed, as well users' needs and requirements. History and logs cover the auditing aspect of the framework. Digital certificates could be used for advanced authentication and encryption. A Public Key Infrastructure is implemented at UCY [79] to ensure the accountability of users and maintain the integrity of the exchanged data. The PKI is still under testing.

### 4.3.9 Business continuity management

This section describes controls relating to business continuity and contingency planning, ranging from analysis and documentation through to regular exercising/testing of the plans. A business continuity management process should be implemented to reduce the disruption caused by disasters and security failures to an acceptable level through a combination of preventative and recovery controls.

The proposed framework addresses a fail safe plan in which it defines that the primary architecture should be replicated so if something happens the secondary infrastructure could take over. The fail safe plan is generic and should be refined to include more details as a guideline to develop a complete business continuity management process.

### 4.3.10 Compliance

The design, operation, use and management of information systems may be subject to statutory, regulatory and contractual security requirements. The organization must comply with applicable legislation such as copyright, data protection, protection of financial data, cryptography restrictions, rules of evidence etc.

The confidentiality documents of the security framework adhere to European and national laws of data protection. Furthermore, a number of European directives were taken into consideration when designing the system such as the e-signatures directive.

### 4.4 Discussion

The proposed security framework that guides DITIS security implementation features, addresses all the fundamental concepts analyzed in ISO/ IEC 17799 standard. Security objectives such as confidentiality, integrity, availability, accountability are adequate addressed, covering the legal, human and technical aspects of the healthcare environment. The aim of the framework was to provide the necessary security mechanisms and procedures that are needed to safeguard the electronic healthcare environment, an objective that is fulfilled.

However, it must be noted that the framework does not provide low level implementation details as this is not its purpose; rather it can be used as a guide to identify what it is needed on a high-level and the user can afterwards look for more details for the area he is interested. Nevertheless, the evaluation process identified areas that could be further analyzed in the security-level information classification scheme, and which are deemed vital in order to provide more details and guidance to the user; security management is essential to provide clear direction and visible management support for security initiatives, that is why it should define the required level of effort allocated under each classification; physical security should be further analyzed with specific measures to prevent unauthorized access and/ or damage to the organization's assets; mobile control access should address issues such as physical protection, cryptographic techniques, backups; and business continuity management should be designed in more detail, defining a combination of preventative and recovery controls to overcome disruption caused by disasters and security failures.

In DITIS, a formal business continuity plan should be created, identifying the key-assets that must be replaced/ recovered when an incident occurs and the procedure that should be followed. Among others, it is important to define the response team, points of contact and the various procedures to recover medical records or replace affected devices. Scenarios should also be designed to aid the recovery planning. Response time is critical to ensure the availability of critical aspects of the system, thus response must

meet the requirements of a specified time frame in which the minimum application and application data must be available.

Furthermore, the evaluation should include a comprehensive and balanced system of measurement which will be used to evaluate performance in information security management and feedback suggestions for improvement. Currently, the ISO/ IEC 17799 does not address performance issues. However, it is vital to assess how implemented security measures affect the performance of the system in terms of latency, consumption of resources (i.e. battery consumption in case of mobile/wireless devices due to computational complexity), and number of successful security incidents that may affect the availability of the system. The aforementioned are performance metrics which affect the effectiveness and efficiency of any system, and most important affect user satisfaction since users require seamless response of the system, especially in the healthcare environment.

# Chapter 5

## Conclusions



### 5.1 Conclusions

Electronic and mobile healthcare applications have revolutionized the healthcare sector, introducing new opportunities, better communication channels and an enhanced quality of care. At the same time, a number of considerations are raised regarding the protection of the most valuable assets processed through these applications; that is the medical records and healthcare transactions. Privacy, confidentiality, integrity, legal and ethical considerations are some of the security challenges that need to be addressed in the healthcare environment.

This research study addressed security-related issues concerning electronic and mobile healthcare systems using DITIS, a telemedicine application. The outcome of the study is a healthcare security framework that includes all the appropriate security technologies and procedures that are needed to safeguard the data, people and infrastructure of the healthcare environment. The framework uses the OCTAVE risk evaluation methodology to identify the risks and areas of concern that address security challenges that should be taken into consideration when implementing security. The security technologies and procedures proposed in the framework are categorized based on the security objective they serve to help people identify the technology they need to implement based on what they want to protect. Finally, the framework defines a security-level information classification scheme that categorizes information based on

its sensitivity (public, internal-use only, confidential, highly confidential). The classification is then associated with the appropriate security technologies that should be considered under each classification level. Labeling information into sensitivity classes aims in helping us provide the appropriate protection by applying the necessary security measures for each situation. The proposed scheme aims in balancing the trade-off between security complexity and performance by providing guidance on the minimum measures/ technologies that are needed to be implemented without complicating the operation of the system or saturating its performance with unnecessary functionality.

The study and the results of this work, has led to the publication of 3 papers. The paper "Security Challenges in a mobile healthcare environment" has been presented in the 3rd International Workshop in Wireless Security Technologies (IWWST) that was organized in London, in 4th of April 2005. The second paper, "E-healthcare Security Framework: DITIS Case Study", was presented in the Tenth International Symposium on Health Information Management Research (iSHIMR2005) organized in Thessalonica, in 23rd of September 2005. Finally, the third paper "Securing Mobile Healthcare Systems using Information Classification: DITIS Case Study" has been presented in the 4th International Workshop on Security in Information Systems that was organized in Cyprus, in 23rd of May 2006.

Electronic healthcare is a sector that will keep evolving in parallel with technological advances. New challenges will arise and need to be addressed, and new approaches should be taken towards healthcare security. Existing solutions and procedures will need to be refined in the new healthcare conditions to keep providing the necessary protection over the information, people and infrastructure in question.

## 5.2 Future work

Future work related with the current study involves extending the proposed security information classification scheme with more technical details. For example define appropriate cryptographic algorithms, how complex passwords should be, how strong physical security should be under each classification level etc. Decisions should be taken based on existing security standards to ensure interoperability with existing and future technology.

Evaluation could be completed as soon as the actual system enters an operational state. A more technical evaluation will be applied using appropriate standards and guidelines such as the Common Criteria [80]; the Common Criteria supports the technical evaluation of IT security features in products. Then, the proposed security framework and the implemented security techniques and procedures in DITIS could be evaluated and result in more detailed findings that will identify the effectiveness of the security framework. The security framework will be refined based on the findings of the evaluation.

Furthermore, the evaluation will assess how the proposed security measures affect the performance of the system. Performance is what often determines the successful adoption of a system. Healthcare applications need, among other things, to quickly respond to users' requests. Wireless devices have a number of limitations that affects performance such as the battery depletion, hardware constrains – small amount of RAM, slow processors and usually no mass storage, and transient communication because of the mobility of the devices the network can experience a high rate of communication failures. All these limitations must be taken into account when choosing security solutions in order to balance complexity with its effect on performance.

Finally, usability is an area that needs more investigation within the security area. Usability is a concept that cannot be overlooked, especially since DITIS system is using wireless devices. Due to the limitations of the size of the wireless devices, all security

solutions implemented that require user input must take into consideration the user's perspective and develop appropriate design for the interface. We do not want users to be resented because the interface is not the intended, and thus it is confusing and time-consuming to use. Instead, the interface regarding the security techniques used, must offer a simple feel and look interface and navigation with minimum clicks that helps the user finish in a short time. Also, technical terminology should be avoided because it is often confusing for non-technical users.

# Chapter 6

## Publications stemming from the thesis

---

6.1 Publications

---

### 6.1 Publications

The outcome of this research study is documented in the following papers:

1. Securing Mobile Healthcare Systems using Information Classification: DITIS Case Study, E. Stavrou, A. Pitsillides, 4th International Workshop on Security in Information Systems, Cyprus, 23 May 2006.
2. e-healthcare Security Framework: DITIS Case Study, E. Stavrou, A. Pitsillides, ISHIMR, 10th International Symposium for Health Information Management Research, Thessaloniki, Greece, 23 Sept 2005.
3. Security Challenges in a Mobile Healthcare Environment, E. Stavrou, A. Pitsillides IWWST (International Workshop in Wireless Security Technologies) Westminster University, London, UK, 4 April 2005.

# References

[1] Eysenbach G., What is eHealth? Journal of Medical Internet Research, 2001

[2] e-Health Communication: e-Health - making healthcare better for European citizens: An action plan for a European e-Health Area, 2004

[3] The Emergence of M –Healthcare, White paper, Ardea Technology Group Inc.

[4] Choudhri A., Kagal L., Joshi L., Finin T., Yesha Y., Patient service: electronic patient record redaction and delivery in pervasive environments, InProceedings, Fifth International Workshop on Enterprise Networking and Computing in Healthcare Industry (Healthcom 2003), June 2003

[5] Misra S., Wickramasinghe N., Goldberg S., Security challenge in a mobile healthcare setting, The 5th Annual Conference of the National Business and Economics Society, Hawaii, March 10-13, 2004

[6] NHS, Report of the review of security at the high security hospitals, 2000

[7] NHS, Share with care! People's view on consent and confidentiality of patient information, 2002

[8] NHS, Good practice guidelines for general practice electronic patient records, 2005

[9] Council framework decision on attacks against information systems, COM, 2002

[10] Directive 95/46/CE issued by the European Parliament and Council on 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data - Official Journal No. L281, 23/11/1995, p. 0031-0050

[11] Directive 2002/58/CE issued by the European Parliament and Council, 12 July 2002, concerning the processing of personal data and the protection of privacy in the Electronic Communications Sector (Directive on privacy and electronic communications) - European Community Official Journal No. 1201/37, 31/07/2002

[12] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)

[13] Directive 1999/93/CE by the European Parliament and Council, 13 December 1999 on a community framework for electronic signatures - Official Journal No. L 013 19/01/2000, p. 0012-0020

[14] Stanford V., Pervasive Healthcare applications face tough security challenges, IEEE Pervasive Computing, 2002

[15] Study on the use of advanced telecommunications services by healthcare establishments and possible implications for telecommunications regulatory policy of the European Union, Empirica and Work Research Center, 2000

[16] Tan J. (editor) e-healthcare information systems, Jossey-Bass publishing, 2005 3

[17] Pietro Di R., Mancini V. L., Security and Privacy Issues of Handheld and Wearable Wireless Devices, Communications of the ACM, Volume 46, Issue 9, 2003

[18] Stavrou E, Pitsillides A. "Security challenges in a mobile healthcare environment", International Workshop on Wireless Security Technologies, UK, 2005

[19] Pitsillides B., Pitsillides A., Samaras G. and Nicolaou M., 'DITIS: Virtual collaborative teams for improved home healthcare', Book Chapter in "Virtual teams: concepts and applications", edited by K.Chandrasekar, ICFAI UNIVERSITY PRESS, 2004

[20] Pitsillides A., Pitsillides B., Samaras G., Dikaiakos M., Christodoulou E., Andeou P. and Georgiades D., DITIS: A collaborative virtual medical team for home healthcare of cancer patients, M-Health: Emerging Mobile Health Systems, (R. H. Istepanian, S. Laxminarayan, C. S. Pattichis, Editors), Kluwer Academic/Plenum Publishers, 2005

[21] Alberts C, Dorofee A. Managing Information Security Risks: The OCTAVE approach, Addison Wesley Publisher, 2002

[22] Alberts C., Dorofee A., OCTAVE Criteria version 2.0, technical report ESC-TR-2001-016, 2001

[23] Alberts C., Dorofee A., OCTAVE Catalog of practices version 2.0, technical report ESC-TR-2001-020, 2001

[24] Martí R, Delgado J., Perramon X., Security Specification and Implementation for Mobile e-Health Services, IEEE International Conference on e-Technology, e-Commerce and e-Service, 2004

[25] Martı R, Delgado J., Perramon X., Network and application security in mobile e-health applications, Networking Technologies for Broadband and Mobile Networks International Conference ICOIN 2004

[26] Dorofee A., Managing Information security risks across the enterprise, Management of Technologies Symposium, 2002

[27] Going mobile: from e-health to m-health, Daou systems white paper, 2001

[28] NSW Department of Commerce, Examples of threats and vulnerabilities, 2003

[29] Rindfleisch T., Confidentiality, Information Technology, and Healthcare, Proceedings of the Second Information Network for Public Health Officials conference, Atlanta, GA, September 1996

[30] EHTA (European Health Telematics Association), Using and sharing health information in the 21st century: A handbook for information governance

[31] Blobel B., ONCONET: A Secure Infrastructure to improve cancer patients' care, European Journal of Medical Research, 2000

[32] Markovic, M., Savic, Z. and Kovacevic, B., Secure mobile health systems: Principles and solutions, in M-Health: Emerging Mobile Health Systems, (Robert H. Istepanian, Swamy Laxminarayan and Constantinos S. Pattichis, Editors), Kluwer Academic/Plenum Publishers, 2004

[33] NSW Department of Commerce, Information security baseline controls, 2003

[34] Huston T., Security issues for implementation of e-medical records, Communications of the ACM, Vol. 44, No. 9, 2001

[35] Guidelines for academic medical centers on security and privacy, ACM/HIPAA workgroup, 2001

[36] Barbera B., Bleumerb G., Daveyc J., Louwersed K., How to achieve secure environments for information systems in medicine, MEDINFO 95, Proceedings, Part 1, International Medical Informatics Association (IMIA), 1995

[37] IATF Chapter 2: Defense in depth, release 3.1

[38] Healthcare Information security, 3COM white paper, 2000

[39] NSW Department of Commerce, Authentication – Digital signatures guideline, 1999

[40] Wohlmacher P., Pharow P., Applications in Health Care using Public-Key Certificates and Attribute Certificates, 16th Annual Computer Security Applications Conference (ACSAC'00), 2000

[41] Bourka, A., Kaliontzoglou, A., Polemi, D., Georgoulas, A. and Sklavos, P. (2003) PKI-based security of electronic healthcare documents, SSGRR 2003 International Conference on Advances in Infrastructure for Electronic Business, Science, Education, Medicine, and Mobile Technologies.

[42] Zhang L., Ahn G., Chu B., A Role-Based Delegation Framework for Healthcare Information Systems, Proceedings of the seventh ACM symposium on Access control models and technologies, 2002

[43] Blobel B., Authorization and access control for electronic health record systems, International Journal of Medical Informatics, 2004

[44] R. C. Barrows, P. D. Clayton, Privacy, Confidentiality, and electronic medical records, Journal of the American Medical Informatics Association, 1996

[45] Christiansen C., Day R., A prescription for healthcare privacy and security, White paper, Computer Associates, 2004

[46] Digital Signature Trust White paper, PKI basics: Digital Signatures and Public Key Infrastructure

[47] Microsoft, Virtual Private Networking in Windows 2000, White paper, 2000

[48] NHS, Confidentiality- Code of practice, 2003

[49] NIST Handbook (1996): An Introduction to Computer Security, Chapter 15: Physical and Environmental Security

[50] Healthcare commission, Policy Handbook: Handling information at the healthcare commission, 2004

[51] Frenzel J., Data security issues arising from integration of wireless access into healthcare networks, Journal of medical systems, 2003

[51] Boran, S. (2003), IT Security Cookbook, Chapter 4: Information Classification

[52] ISO17799 Security Standard, Section 5: Asset Classification and Control

[53] CSTB - Computer Science and Telecommunications Board Commission on Physical Sciences, Committee on Maintaining Privacy and Security in Health Care application (1997), For the Record: Protecting Electronic Health Information, National Academy Press, pg. 94-96

[54] Krutz R., R. D. Vines, The CISSP Prep Guide: Mastering the ten domains of computer security, Wiley Computer publishing, 2001

[55] Bell, D.E., and LaPadula, L.J. Secure computer system: unified exposition and Multics interpretation. MTR-2997, MITRE Corp., Bedford, MA, March, 1976

[56] Biba K. J. Integrity Constraints for Secure Computer Systems, Technical Report ESD-TR76-372, USAF Electronic System Division, Bedford, Massachusetts, April 1977

[57] Brewer D.F.C. and Nash M.J., The Chinese Wall Security Policy, Proceedings of the IEEE Symposium on Security and Privacy, Oakland, May 1989, pp. 206-214.

[58] Graham, G. and Denning, P. Protection: Principles and Practices, In Proceedings of the AFIPS Spring Joint Computer Conference. 1972, pp 417-429

[59] Spinellis D., Gritzalis S., Iliadis J., Gritzalis D., and Katsikas S. Trusted third party services for deploying secure telemedical applications over the WWW, *Computers and Security*, 18(7):627–639, 1999

[60] Reid, P., Biometrics for Network Security, Prentice Hall, 2003

[61] McLean J., The specification and modelling of computer security, IEEE Computer, 1999

[62] B. Cohen, A formal model of healthcare security policy, City University, 1996

[63] Anderson J. R, Healthcare Protection Profile – Comments, Cambridge University

[64] ISO/IEC 17799 Information technology - Security techniques - Code of practice for information security management

[65] Center for Medicare & Medicaid Services (CMS), HIPAA Security Series

[66] Stavrou E., Pitsillides A., e-healthcare Security Framework: DITIS Case Study, ISHIMR, 10th International Symposium for Health Information Management Research, Thessaloniki, Greece, Sept 2005

[67] Stavrou E., Pitsillides A., Securing Mobile Healthcare Systems using Information Classification: DITIS Case Study, 8th International Conference on Enterprise Information Systems, Cyprus, May 2006

[68] Anderson R., Security in clinical information systems. BMA Report, British Medical Association, Jan 1996, ISBN 0-7279-1048-5

[69] Anderson R., A security Policy Model for clinical information systems. In Proceedings of the IEEE Symposium on Research in Security and Privacy, Research in Security and Privacy, pp. 30–43. IEEE Computer Society, Technical Committee on Security and Privacy, IEEE Computer Society Press, Oakland, CA, May 1996

[70] Bishop M., Introduction to computer security, Addison-Wesley publishing, 2005

[71] NIST Handbook (1996): An Introduction to Computer Security, Chapter 9: Assurance

[72] RFC 2196 Site security handbook

[73] Eastton C., Network defense and countermeasures – Principles and practices, Pearson Prentice Hall, 2006

[74] HandHeldMed Patient Tracker Products,
http://www.patienttracker.com/products.htm

[75] Wireless Medicenter, http://www.wirelessmedicenter.com/mc/glance.cfm

[76] David Brazier, Alpha Bravo Charlie Ltd, The m-care project, http://www.m-care.co.uk/tech.html

[77] PatientKeeper, http://www.patientkeeper.com/products.html

[78] PocketMD, http://www.pocketmd.com

[79] Ευαγγέλου Χ., Υποδομή Δημόσιου Κλειδιού – Ανάπτυξη της Αρχής Πιστοποίησης "Ιπποκράτης"

[80] Common Criteria for Information Technology Security Evaluation

# Appendix A: Security Policies

Security policies are the cornerstone of any effective security strategy. They are used to complement and support the operation of a variety of security solutions. A well written security policy provides guidelines to employees as to how to maintain security of the organization's data and systems. All employees must follow the suggested procedures otherwise they may face penalties based on the violation they commit.

Based on DITIS profile, we have identified a number of security policies that are applicable to be implemented in DITIS environment. This section provides the general template of each security policy; the actual policies will be finalized when DITIS reaches an operational level.

1. **Password Policy**

Strong, secure passwords are the cornerstone of an effective security strategy. They are the front line of protection for user accounts. Passwords ensure that only authorized personnel will be able to gain access to a system or network. A poorly chosen password may result in the compromise of the company's entire corporate network. As such, all employees are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Passwords are used for various purposes at the corporation. Some of the more common uses include: user level accounts, web and email accounts, screen saver protection, etc. Everyone should be aware of how to select strong passwords in order to protect the systems and the information that reside at the company.

- Passwords must contain at least eight nonblank characters.
- Passwords must contain a combination of letters (preferably a mixture of upper and lowercase letters), numbers, and at least one special character within the first seven positions.

- Passwords must contain a nonnumeric letter or symbol in the first and last positions.
- Passwords must not contain the user login name.
- Passwords must not include the user's own or close friend's or relative's name, employee number, Social Security number, birthdate, telephone number, or any information about him or her that the user believes could be readily learned or guessed.
- Passwords must not include common words from an English dictionary or a dictionary of another language with which the user has familiarity.
- Passwords must not contain commonly used proper names, including the name of any fictional character or place;
- Passwords must not contain any simple pattern of letters or numbers such as "qwertyxx".
- Passwords must be changed at least every 40 days.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- Password should remain confidential and unique.
- Do not use the same password for company's accounts as for other non-company's access.
- In the case of login failure, the user has three opportunities to provide the correct login and password. If he doesn't, the account gets disable and he must contact the network administrator.

**2. Anti-virus policy**

All employees must follow recommended processes in order to prevent virus problems and protect the assets of the organization:

- Always run the supported anti-virus software. Download and install anti-virus software updates as they become available.
- Schedule the anti-virus to run daily at a time when there is no activity (i.e. over night)

- Avoid direct opening or executing e-mail attachments. Always save the email attachment and scan for viruses before reading or executing them.
- Always scan a floppy diskette from an unknown source for viruses before using it.
- Back-up critical data and systems configurations on a regular basis and store the data in a safe place.
- If an installation of a new program conflicts with anti-virus software, run the anti-virus utility to ensure a clean machine, disable the software, then run the program. After the installation, enable the anti-virus software. When the anti-virus software is disabled, do not run any applications that could transfer a virus, e.g., email or file sharing.

## 3. Encryption policy

Encryption is the primary mean for providing confidentiality services for information sent over the Internet. Encryption can be used to protect any electronic traffic, such as mail messages or the contents of a file being downloaded. Encryption also can protect information in storage, such as in databases or stored on computer systems where physical security is difficult or impossible.

Therefore, encryption must be used to protect any electronic traffic exchanged between the company and its customers.

- Any remote connection to the organization's network must be established through VPN channels.
- If for any reason, an employee has to send confidential information via email, he must do so by configuring his email application to encrypt the message.
- The organization must implement an appropriate encryption service and provide it to employees when they are using the healthcare application to send or retrieve confidential information.
- Sensitive information that is locally stored on mobile devices must be encrypted.

4. **Audit policy**

Auditing is an important component for maintaining the organization's security, since it can help investigate possible security incidents and ensure conformance to the organization's security policies. An audit policy should balance between auditing enough events to be effective, but not so many events that the ones that really matter get lost.

The auditing may include a variety of events. These events fall into several categories. It is up to the personnel who perform the audit to decide which events will be monitor. The following list includes such events:

- ***Account Login*** - An event that's triggered when a domain controller receives a login request. You can audit an account login based upon successful logins or login failures.
- ***Account Management*** - Pertains to any sort of maintenance to user accounts. For example, if a user creates, renames, or deletes a user account, an event can be logged.
- ***Logon Events*** - Login Events refer to any time any user logs in or out of the system. In some situations, Login Events may also be triggered when a user connects to or disconnects from a computer on the network.
- ***Object Access*** - Object Access tracks the way that users access physical objects such as files, folders, and printers.
- ***Policy Change*** - Perhaps one of the most important types of event category. These events are triggered when someone makes a change to your security policies. These changes may include anything from changing user rights to changing audit policies.
- ***Privilege Use*** - The Privilege Use category of events can be used to make an event log entry any time that someone uses one of the special rights you've assigned to them.

- ***System Events*** - Events going on within the physical system. For example, you can log each time a server (or workstation) is shut down or restarted. A system event can also be triggered if the security log fills up.

Some recommendations, concerning the management of audit trails, are given below:

1. Protect the audit trail so that no normal user can view or modify the audit log.
2. Do not allow multiple logons. If an employee is allowed to logon to his/her workstation and then walk around the corner and logon to another workstation with the same logon ID and password, the audit trail can no longer track the user as precisely as security needs require. If both terminals are active with the same logon, the system can never be sure if the authorized user is on the system or if someone else is using his/her account.
3. Review audit logs for security-related incidents on a regular basis.
4. Ensure that all users know that their systems and their actions are being monitored.
5. Provide all users of the system with "security alert" announcements.

## 5. Security incident handling policy

An incident is defined as an event that has actual or potentially adverse effects on computer or network operations resulting in fraud, waste, or abuse; compromise of information; or loss or damage of property or information.

Security incidents can, for example, be triggered by user errors which result in loss of data or alteration of sensitive system parameters, the appearance of security loopholes in hardware or software components, and exploitation of technical vulnerabilities, large-scale infection by computer viruses, hacking of Internet servers, disclosure of confidential data, and many more.

A security incident could cause significant loss or damage. To prevent or contain any loss or damage, security incidents should be dealt with swiftly and efficiently. If there is

a predefined procedure available to be invoked, then reaction times can be minimized. The possible loss or damage which could occur in a security incident can affect both the confidentiality and integrity of data and also its availability.

The purpose of this guideline is to ensure an efficient and effective response to computer security incidents. A poorly handled incident can result in wasted time, conflicting information and negative publicity.

General

Handling of security incidents should be aimed at ensuring the following:

- The ability to respond so that security incidents and security problems are detected and reported to the appropriate responsible person(s) promptly.
- The ability to decide whether it is a local security problem or constitutes a security incident.
- The ability to take action so that in the event of a security incident the necessary measures can be taken and implemented at short notice
- Minimization of damage (this is achieved through prompt notification of any other parts of the organization which could be affected), and
- Effectiveness (this is achieved by practicing and monitoring the capability to handle security incidents)

Notification and points of contact

Each user of the corporation has a responsibility to report incidents that constitute a security incident or violation of the company's policies. All security incidents will be reported to the appropriate office as soon as an incident comes to the attention of an employee or other person charged with responsibility for information resources within the company. An appropriate contact list must be defined and distributed within the organization so that people know who to contact in the case of an incident. The following template could be used to define the contact list:

- Security incident team (if any) [a team composed of IT administrators, IT users, Public Relations Staff and possibly Management]
<Names> <Telephone numbers> <Emails> or
- System manager/administrator <His/her name> <Telephone number> <Email>
- Technical manager <His/her name> <Telephone number> <Email>
- System owner <His/her name> <Telephone number> <Email>
- Legal counsel (if appropriate) <His/her name> <Telephone number> <Email>

If for any reason the employee is unable to contact any of the above people and he believes that his computer has been broken into, he should physically unplug the computer from the network until a security engineer can look at it. However, it is important not to shut the computer down or kill any processes if at all possible since evidence may exist that is useful to identify what happened and also help prevent future attacks.

Identifying an incident

This stage involves determining if a problem really exists. To assist in identifying whether there really is an incident, it is usually helpful to obtain and use any detection software that may be available. In addition, there are certain indications or "symptoms" of an incident that deserve special attention:

- System crashes
- New user accounts, or high activity on a previously low usage account
- Changes in file lengths or dates
- Data modification or deletion
- Denial of service
- Unexplained, poor system performance
- System anomalies
- Suspicious browsing
- Inability of a user to log in due to modifications of his/her account

This list is comprehensive; it includes a number of common indicators. It is best to collaborate with other technical and computer security personnel to make a decision as a group about whether an incident is occurring.

Key steps

- Containment

The purpose of containment is to limit the extent of an attack. An essential part of containment is decision making (e.g., determining whether to shut a system down, disconnect from a network, monitor system or network activity, set traps, disable functions such as remote file transfer, etc.).

- Eradication

Once the incident has been contained, it is time to eradicate the cause. But before eradicating the cause, great care should be taken to collect all necessary information about the compromised system(s) and the cause of the incident as they will likely be lost when cleaning up the system. Software may be available to help you in the eradication process, such as anti-virus software.

- Recovery

Once the cause of an incident has been eradicated, the recovery phase defines the next stage of action. The goal of recovery is to return the system to normal. If an incident turns out to be a successful break-in, then the system must be kept off the network until it has been evaluated by a security engineer and all corrective action has been taken. The following is a partial list of cleanup procedures that a security engineer may require:

1. Re-installation of the operating system: If it's clear that a cracker gained full access to a system and could have modified the operating system, then the operating system will have to be re-installed from original (CD-ROM) media.
2. Re-authentication of all users: If it's clear that one or more user accounts have been compromised, then all users on the system will have to be re-authenticated. This is done by first disabling all accounts and then requiring each user to contact the system administrator personally to re-enable their account and select a new password.
3. Scanning the password file for "bad" passwords: Software is available to search for "bad" or easily guessed passwords. The security engineer may require that this software be run, then each account found to have a bad password will be re-authenticated.
4. Installation of security patches or software: The security engineer may require that additional security software be installed and/or that existing software be patched or updated.

- Follow-up

Once you believe that a system has been restored to a "safe" state, it is still possible that holes, and even traps, could be lurking in the system. One of the most important stages of responding to incidents is also the most often omitted, the follow-up stage. In the follow-up stage, the system should be monitored for items that may have been missed during the cleanup stage.

- Aftermath-lessons learned

In the wake of an incident, several actions should take place. These actions can be summarized as follows:

1. An inventory should be taken of the systems' assets, (i.e., a careful examination should determine how the system was affected by the incident).
2. The lessons learned as a result of the incident should be included in revised security plan to prevent the incident from re-occurring.

3. A new risk analysis should be developed in light of the incident.
4. An investigation and prosecution of the individuals who caused the incident should commence, if it is deemed desirable.

## 6. Server security policy

The purpose of this policy is to establish standards for the base configuration of internal server equipment that is owned and/or operated by the organization. Effective implementation of this policy will minimize unauthorized access to the organization's proprietary information and technology.

All internal servers deployed must be owned by an operational group that is responsible for system administration. Approved server configuration guides must be established and maintained by each operational group, based on business needs. Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment.

- Servers must be registered within the corporate enterprise management system. At a minimum, the following information is required to positively identify the point of contact:
  - Server contact(s) and location, and a backup contact
  - Hardware and Operating System/Version
  - Main functions and applications, if applicable
- Information in the corporate enterprise management system must be kept up-to-date.
- Configuration changes for production servers must follow the appropriate change management procedures.
- Services and applications that will not be used must be disabled where practical.
- Access to services should be logged and/or protected through access-control methods such as TCP Wrappers, if possible.

- The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.
- Always use standard security principles of least required access to perform a function.
- Do not use root when a non-privileged account will do.
- If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).
- Servers should be physically located in an access-controlled environment.
- Servers are specifically prohibited from operating from uncontrolled work areas.

# Appendix B: Confidential Documents

In order to comply with European and national legislation of Data Protection, appropriate documents were created and distributed among DITIS patients, medical professionals, administrative staff and software developers.

The patients are informed about the need to process their medical information and give their written consent; medical professionals, administrative staff and software developers acknowledge their responsibility to protect the privacy of sensitive information and use it only to perform their assigned duties.

Following, are the documents created to support the protection of information confidentiality according to the Data Protection Law guidelines.

# ΕΝΤΥΠΟ ΣΥΓΚΑΤΑΘΕΣΗΣ

## ΓΙΑ ΕΠΕΞΕΡΓΑΣΙΑ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΣΑΣ ΔΕΔΟΜΕΝΩΝ ΑΠΌ ΤΟΝ ΠΑΓΚΥΠΡΙΟ ΣΥΝΔΕΣΜΟ ΚΑΡΚΙΝΟΠΑΘΩΝ ΚΑΙ ΦΙΛΩΝ (ΠΑ.ΣΥ.ΚΑ.Φ)

Έχουμε νομική υποχρέωση δυνάμει του Νόμου για την Επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα (Προστασία του Ατόμου) να διασφαλίζουμε ότι η φύλαξη και η επεξεργασία των προσωπικών σας δεδομένων και όλων των άλλων πληροφοριών που σχετίζονται με την υγεία σας, συμμορφώνονται με τις προϋποθέσεις του Νόμου.

Τέτοια προσωπικά δεδομένα συμπεριλαμβάνουν πληροφορίες που έχουν δοθεί ή θα δοθούν στο μέλλον:

- Από εσάς κατά την εγγραφή σας, κατά την εξέταση σας από τον ιατρό και γενικά κατά την περίθαλψη σας,
- ή έχουν εξασφαλιστεί από τρίτους όπως π.χ. παραπεμπτική, αποτελέσματα εξετάσεων ή εκθέσεις άλλων ιατρών.

Αποδέκτες των πληροφοριών αυτών είναι όλοι οι εξουσιοδοτημένοι και κατάλληλα εκπαιδευμένοι στο χειρισμό των πληροφοριών υπάλληλοι του ΠΑ.ΣΥ.ΚΑ.Φ.

Σύμφωνα με το Νόμο, πληροφορίες που σχετίζονται μεταξύ άλλων, με την υγεία ή την εθνική προέλευση, θεωρούνται Ευαίσθητα Δεδομένα. Οι πληροφορίες αυτές μπορούν να χρησιμοποιηθούν μόνο με τη ρητή σας συγκατάθεση.

---

## ΕΧΕΜΥΘΕΙΑ

Σύμφωνα και με τις πρόνοιες του Νόμου όλες οι προσωπικές σας πληροφορίες θα τηρούνται απόρρητες και θα τυγχάνουν εμπιστευτικής μεταχείρισης. Οποιαδήποτε πληροφορία σας αφορά δε θα αποκαλύπτεται σε τρίτα πρόσωπα, εκτός στις περιπτώσεις που ο Νόμος το επιτρέπει. Οι περιπτώσεις αυτές είναι:

- Όταν η αποκάλυψη γίνεται με δική σας γραπτή συγκατάθεση,
- Όταν η αποκάλυψη γίνεται διότι αυτό απαιτείται από το Νόμο ή δικαστικό διάταγμα,
- Όταν η αποκάλυψη γίνεται στα πλαίσια δικαστικής διαδικασίας μεταξύ μας,
- Όταν η αποκάλυψη γίνεται για σκοπούς τήρησης και λειτουργίας του Αρχείου Καρκίνου.

## ΑΣΦΑΛΕΙΑ ΤΩΝ ΔΕΔΟΜΕΝΩΝ

Ο ΠΑ.ΣΥ.ΚΑ.Φ. θα λαμβάνει κάθε αναγκαίο τεχνικό ή οργανωτικό μέτρο για την ασφάλεια των δεδομένων και την προστασία τους από τυχαία ή αθέμιτη καταστροφή, τυχαία απώλεια, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση και κάθε άλλη αθέμιτη επεξεργασία.

## ΧΡΗΣΗ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΣΑΣ ΔΕΔΟΜΕΝΩΝ

Θα φυλάττουμε και θα επεξεργαζόμαστε τα προσωπικά σας δεδομένα σε φυσική μορφή ή στους ηλεκτρονικούς υπολογιστές του ΠΑ.ΣΥ.ΚΑ.Φ. και θα τα χρησιμοποιούμε για τους ακόλουθους σκοπούς:

- Παροχή των υπηρεσιών μας.
- Έρευνα και στατιστική ανάλυση. Οι προσωπικές σας πληροφορίες είναι δυνατό να χρησιμοποιηθούν για να μελετήσουμε ατομικές ανάγκες και τάσεις με σκοπό να βελτιώσουμε τις υπηρεσίες που προσφέρουμε.

# ΔΙΚΑΙΩΜΑ ΠΡΟΣΒΑΣΗΣ ΣΤΑ ΔΕΔΟΜΕΝΑ ΠΡΟΣΩΠΙΚΟΎ ΧΑΡΑΚΤΗΡΑ ΚΑΙ ΥΠΕΥΘΥΝΟΣ ΕΠΕΞΕΡΓΑΣΙΑΣ

Η πιο πάνω πληροφόρηση για τους σκοπούς και τη χρήση των Προσωπικών σας Δεδομένων καλύπτει τις υποχρεώσεις μας με βάσει το Νόμο για την Επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα (Προστασία του Ατόμου).

Σύμφωνα με τις πρόνοιες του Νόμου, έχετε δικαίωμα πρόσβασης στις λεπτομέρειες που έχουμε καταγράψει για σας, έναντι πληρωμής του σχετικού δικαιώματος και φυσικά έχετε δικαίωμα αντίρρησης και διόρθωσης τηρουμένων πάντοτε των σχετικών προνοιών του Νόμου.

Ευελπιστούμε ότι η πληροφόρηση που περιέχεται στο έγγραφο αυτό θα σας είναι χρήσιμη. Αν έχετε οποιεσδήποτε ερωτήσεις ή ανησυχίες, μη διστάσετε να επικοινωνήσετε με τον ΠΑ.ΣΥ.ΚΑ.Φ. που είναι ο **Υπεύθυνος Επεξεργασία**ς:

ΠΑ.ΣΥ.ΚΑ.Φ.
Φωτεινού Πανά 12-14
Παλλουριώτισσα
1045 Λευκωσία
Τηλ: +357 (22) 345444
Φαξ: +357 (22) 346116

# ΔΗΛΩΣΗ

Με την υπογραφή σας στο έγγραφο αυτό βεβαιώνετε ότι:

- Έχετε διαβάσει και ενημερωθεί για το περιεχόμενο της δήλωσης αυτής και δίδετε ελεύθερα και με πλήρη επίγνωση τη ρητή συγκατάθεση και αποδοχή σας για τη νόμιμη επεξεργασία των προσωπικών σας δεδομένων συμπεριλαμβανομένων των ευαίσθητων δεδομένων για τους σκοπούς που περιγράφονται πιο πάνω.
- Συμφωνείτε ότι το Αρχείο Καρκίνου θα έχει πρόσβαση και δικαίωμα επεξεργασίας των δεδομένων που σας αφορούν.
- Συμφωνείτε ότι ευαίσθητα δεδομένα που έχουμε συλλέξει θα τύχουν επεξεργασίας για την υποστήριξη των υπηρεσιών μας.

Υπογραφή: _____ Ημερομηνία: _____

Μάρτυρας: _____

# Code of Ethics for professionals handling confidential medical information for the Cyprus Association of Cancer Patients and Friends (PA.SY.KA.F.)

I _____

of _____

hereby understand the significance and agree to protect any confidential information accessed on behalf of PA.SY.KA.F. while using DITIS (ΔΙΤΗΣ stands for "Δίκτυο Ιατρικής Τηλεσυνεργασίας", i.e. Network for Medical Collaboration) or other means, as required by the laws of the Cypriot Government and the European Community. I understand that any disclosure of confidential information is both unethical and illegal.

Therefore, during my involvement with DITIS, I shall:

1. Use the information provided only for the purpose of my job function and for a legitimate cause.
2. Not reveal confidential information to unauthorized people who are not concerned with the subject.
3. Be considered liable in the case where I am found compromising any sensitive information.

Signed By: _____

Date: _____

Witnessed By:_____

Witnessed By:_____